Biochemical and chemical methods of key derivation for cryptographic ciphers

Leif K. Mcgoldrick

University at Albany, State University of New York, dekuleif@gmail.com

The University at Albany community has made this article openly available. Please share how this access benefits you.

Follow this and additional works at: https://scholarsarchive.library.albany.edu/legacy-etd

Part of the Analytical Chemistry Commons, and the Biochemistry Commons

Recommended Citation

https://scholarsarchive.library.albany.edu/legacy-etd/2519

This Dissertation is brought to you for free and open access by the The Graduate School at Scholars Archive. It has been accepted for inclusion in Legacy Theses & Dissertations (2009 - 2024) by an authorized administrator of Scholars Archive. Please see Terms of Use. For more information, please contact scholarsarchive@albany.edu.
Biochemical and Chemical Methods of Key Derivation for Cryptographic Ciphers

By

Leif K. McGoldrick

A Dissertation

Submitted to the University at Albany, State University of New York

In Partial Fulfillment of

The Requirements for the Degree of

Doctor of Philosophy

College of Arts and Sciences

Department of Chemistry

2020
Table of Contents

Biochemical and chemical methods of key derivation for cyphers in cryptography.................. i

Acknowledgements ........................................................................................................ vi

Abstract ......................................................................................................................... viii

Prefatory Information...................................................................................................... x

Copyright Permissions .................................................................................................... x

List of featured manuscripts.......................................................................................... x

Ethics Statement ............................................................................................................. xi

List of Abbreviations...................................................................................................... xi

List of Tables .................................................................................................................... xiv

List of Equations ............................................................................................................. xv

List of Schemes ............................................................................................................... xvi

List of Figures ................................................................................................................. xviii

Chapter 1. Introduction .................................................................................................. 1

1.1 Theory of Bioaffinity-based Assays and Ultraviolet-Visible Spectroscopy ............ 1

1.1.1 Bioaffinity-Based Assays.................................................................................... 1

1.1.2 Enzymatic Assays .............................................................................................. 1

1.1.3 Immunoassay ...................................................................................................... 2

1.1.4 Ultraviolet Visible Spectrophotometry (UV-Vis)............................................. 3

1.2 Cybersecurity, Ciphers, and Encryption................................................................. 4
3.3 Results and Discussion .................................................................................................................. 31
  3.3.1 Reproducibility and variation check ......................................................................................... 31
  3.3.2 Encryption and Decryption ........................................................................................................ 32
  3.4 Conclusion ................................................................................................................................... 33

4. Immunoassay Encryption .................................................................................................................. 36
  4.1 Introduction .................................................................................................................................... 36
  4.2 Materials and Methods .................................................................................................................. 37
    4.2.1 Chemicals ................................................................................................................................. 37
    1.2.2 Immunoassay ........................................................................................................................... 38
    4.2.3 Cipher ....................................................................................................................................... 38
  4.3 Results and Discussion .................................................................................................................... 40
    4.3.1 Reproducibility and variation check ......................................................................................... 40
    4.3.2 Encryption ............................................................................................................................... 40
    4.3.3 Decryption ............................................................................................................................... 42
  4.4 Conclusion ....................................................................................................................................... 42

5. Biometrics for Asymmetric Cipher .................................................................................................... 44
  5.1 Introduction ...................................................................................................................................... 44
  5.2 Materials and Methods .................................................................................................................. 45
    5.2.1 Chemicals .................................................................................................................................... 45
    5.2.2 Enzymatic Assays ..................................................................................................................... 46
Acknowledgements

I would like to thank the Department of Chemistry at the University at Albany, State University of New York and my research advisor, Dr. Jan Halámek. They have allowed me to further my pursuit of my goals. I am also thankful to my doctoral committee members, Professor Maksim Royzen, Professor Jeremy Feldblyum, and Professor Jia Sheng, for their time and knowledge.

I would also like to thank the members of the Halámek research lab: Juliana Agudelo, Crystal Huynh, Erica Brunelle, Mindy Hair, Cheyenne Bowman, Alyssa Shoemaker, Morgan Eldridge, Hailey Marini, Henry Hance, Audrey Auleley, Elizabeth Weiss, and Giana Biddle. In addition, I would like to thank the undergraduate student who helped me on a few of my early projects, Sarah Farrell. These wonderful people have not only provided fantastic support on research projects and manuscript papers but also made daily life enjoyable.

I would especially like to thank my family and friends for their unending support throughout my life. My parents have always supported me in so many ways from the beginning: sending me to respected schools, helping me achieve my goals, and providing advice and guidance that made me who I am today. Also, all the home cooked food they would bring up whenever they visited. My friends, both in Albany and back in Philadelphia, have helped me greatly throughout this process as well. I would especially like to thank Tim and Steph Muzio, the two people who have been my best friends since I started at UAlbany, for their continual support and friendship. To my other friends in Albany who were always there to listen: Dan Tedesco, Mindy Hair, Marisia Fikiet, and Cameron Longo, I cannot thank you enough. From Philadelphia, I would like to thank Joe Lauman, who not only was there to lend an ear but also provided ample knowledge and support for my projects from a computer science perspective. To my friend group from undergraduate;
Megan Van Vliet, Keyan West, Mary Sexton and Ryan Charlton; thank you for all of your help both inside and outside of school, you are all truly irreplaceable.
Abstract

Cryptography is a vital component of digital communication and digital data in general. The use of cryptography is necessary to support the veracity of data and to protect it from outside parties with malicious intent. Cryptography focuses on two main facets that are vital for this goal: data encryption and user authentication. Encryption protects the data by transforming it into an encrypted text that would not allow someone access without having or breaking the encryption method that was used to make it. User authentication is a multiple part process that allows for one to be able to identify oneself to prove they were the actual sender of a message.

As the processes used for encryption have developed throughout the years, cryptologists have mainly focused on employing the use of ciphers, a character-by-character transformation of data, for high security encryption. For ciphers to work, one requires to possess the encryption key for encryption and a corresponding decryption key for decryption. The work presented in this dissertation focuses on the derivation of these keys through multiple biochemical and chemical methodologies combined with multiple types of cryptographical cipher systems.

The requirements for a key through this process are that it needs to be reproducible, but also variable for subsequent keys. For general message encryption, both the encryption and decryption keys are the exact same, as a symmetrical-key cipher system, which requires the results of the experiments performed to be reproducible. Since both the sender and the receiver will be performing the same experiment, the reproducibility of the results is paramount. For these ciphers, a rule is that you do not want to use a key more than once for any subsequent message and to use novel keys for the highest level of security as it is easier to break the cipher if a key is used multiple times\textsuperscript{1–3}. To this end, it is important that the key derivation methodology is variable for subsequent experiments to produce novel keys each time by changing the chosen parameters.
Currently, the procedure used for the derivation of keys involves a random number generators (RNGs) or the message sender’s own parameters. However, there are many issues with random number generators with encryption and with their function in general. The research here presents a worthwhile alternative to these RNGs by utilizing biochemical and chemical methodologies as the source for cryptographic keys. In this research, one chemical method is presented in addition to three biochemical methods for various cryptographic ciphers. The biochemical methods involve bioaffinity-based assays with colorimetric responses to produce a signal. The chemical method relies on electrochemical methods to produce data. Three of the methods presented in this dissertation utilize symmetrical-key ciphers, which purely focus on data encryption. For these, a basic addition/subtraction-based cipher is used for the first, and all subsequent experimentation relies on the cipher used as the current standard for encryption today. The final method relies on the use of biomarkers in sweat to produce keys for asymmetrical-key cryptography, which can perform both data encryption and user authentication functions.
Prefatory Information

Copyright Permissions

The research presented in the documents was conducted primarily by Leif K. McGoldrick in partial fulfillment pertaining to the requirements by the University at Albany, SUNY, and the Department of Chemistry for a Doctor of Philosophy (Ph.D.) in Chemistry. All 4 research sections of this dissertation were adapted in part from scientific manuscripts wherein Leif K. McGoldrick was the first author, demonstrating the experimental work described within this document is either published or in the process of submission. Copyright permissions were acquired for the inclusion of previously published work and are included in the Appendix.

List of featured manuscripts

2. Chapter 3 was adapted in part from McGoldrick, L. K., Halápek, J. “Encryption and Decryption with Symmetrical Keys Utilizing Redox Reaction via Advanced Encryption Standard” Manuscript in Preparation.
3. Chapter 4 was adapted in part from McGoldrick, L. K., Halápek, J. “AES Encryption Utilizing Cryptographic Keys Derived from Immunoassay”. Manuscript in Preparation.
Ethics Statement

As shown by Mindy E. Hair, the Institutional Review Board, Office of Pre-Award and Compliance at the University at Albany have approved each of the experimental protocols described in this manuscript. For these studies, male and female volunteers provided their sweat for analysis of two compounds: lactate and urea. For each study, all volunteers were required to sign a document that stated any potential risks associated with their participation in each study. This document also states that the volunteers will not receive any benefits such as compensation for their participation. Lastly, the volunteers were informed that no personal information was used as part of this study with the exception of the small molecule levels within their sweat.

List of Abbreviations

ΔAbs change in absorbance

λ_{max} maximum wavelength

°C degrees Celsius

µL microliter

µM micromolar

Abs Absorbance

ABTS 2,2’-azino-bis(3-ethylbenzothiazoline-6-sulfonic acid)

AC-DC Alternating Current/Direct Current

AES Advanced Encryption Standard

Ag Silver
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AgCl</td>
<td>Silver chloride</td>
</tr>
<tr>
<td>ALP</td>
<td>Alkaline Phosphatase</td>
</tr>
<tr>
<td>bit</td>
<td>basic unit of digital information. 8 bits=1 byte</td>
</tr>
<tr>
<td>BSA</td>
<td>Bovine Serum Albumin</td>
</tr>
<tr>
<td>byte</td>
<td>unit of digital information</td>
</tr>
<tr>
<td>ct</td>
<td>Ciphertext</td>
</tr>
<tr>
<td>DC</td>
<td>Direct Current</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
</tr>
<tr>
<td>E.C.</td>
<td>Enzyme Commission Number</td>
</tr>
<tr>
<td>EKG</td>
<td>Electrocardiogram</td>
</tr>
<tr>
<td>ELISA</td>
<td>Enzyme-Linked Immunosorbent Assay</td>
</tr>
<tr>
<td>GlDH</td>
<td>Glutamate Dehydrogenase</td>
</tr>
<tr>
<td>H&lt;sub&gt;2&lt;/sub&gt;O&lt;sub&gt;2&lt;/sub&gt;</td>
<td>Hydrogen Peroxide</td>
</tr>
<tr>
<td>HCl</td>
<td>Hydrochloric Acid</td>
</tr>
<tr>
<td>hex</td>
<td>hexadecimal numerical system</td>
</tr>
<tr>
<td>HgG</td>
<td>Human Gamma Globulin</td>
</tr>
<tr>
<td>HRP</td>
<td>Horseradish Peroxidase</td>
</tr>
<tr>
<td>kRSA</td>
<td>Kid RSA</td>
</tr>
</tbody>
</table>
KTG  \( \alpha \)-ketoglutarate

LOx  Lactate Oxidase

mL  milliliter

mM  millimolar

mod  modulo operation

n  number of trials

NAD\(^+\)  Nicotinamide Adenine Dinucleotide

NADH  \( \beta \)-Nicotinamide Adenine Dinucleotide Reduced

nm  nanomolar

pNP  para-Nitrophenol

pNPP  para-Nitrophenylphosphate

RSA  Rivest-Shamir-Adleman public key cryptosystem

TMB  3,3',5,5'-Tetramethylbenzidine

UR  Urease

UV-Vis  Ultraviolet-Visible

XOR  exclusive or binary operation
List of Tables

Table 2.1  Public alphanumeric cipher table .......................................................... 18
Table 2.2  message transformation ................................................................. 18
Table 2.3  Example of a possible set of parameters that would be in the “manual” for both the sender and receiver .................................................. 19
Table 3.1  Current at select potentials that is to be used to create the encryption key ...... 33
Table 3.2  Encryption and decryption process steps through AES .......................... 33
Table 4.1  Encryption Process utilizing ELISA data ........................................... 41
Table 4.2  Decryption Process utilizing ELISA data ........................................... 42
Table 5.1  Biometric Data for Individual 1 (Bob) .............................................. 49
Table 5.2  kRSA values for Individual 1 (Bob) .................................................. 49
Table 5.3  Biometric Data for Individual 2 (Alice) ........................................... 51
Table 5.4  kRSA values for Individual 2 (Alice) .............................................. 51
List of Equations

Equation 1.1  
Absorbance and %Transmittance .........................................................3

Equation 1.2  
Beer-Lambert Law .................................................................3

Equation 3.1  
reduction reaction of ferricyanide to ferrocyanide .............................28

Equation 3.2  
oxidation reaction of ferrocyanide to ferricyanide ...........................28

Equation 5.1  
calculation of M for kRSA ..............................................................49

Equation 5.2  
calculation of e for kRSA ..............................................................49

Equation 5.3  
calculation of d for kRSA ..............................................................49

Equation 5.4  
calculation of d for kRSA ..............................................................49

Equation 5.5  
kRSA message encryption ..............................................................50

Equation 5.6  
kRSA message decryption ..............................................................50

Equation 5.7  
kRSA signature encryption ..............................................................51

Equation 5.8  
kRSA signature encryption ..............................................................51
List of Schemes

Scheme 1.1 Enzymatic assay example………………………………………………………. 1

Scheme 1.2 Enzyme-linked immunosorbent assay example……………………………… 2

Scheme 1.3 A basic symmetrical-key encryption system…………………………………. 6

Scheme 1.4 Asymmetrical-key encryption of a message……………………………………... 8

Scheme 1.5 Asymmetrical-key encryption for authentication……………………………… 8

Scheme 2.1 A general scheme depicting symmetrical-key cipher-based encryption showing how a bioaffinity-based enzymatic assay system would be incorporated into the process……10

Scheme 2.2 The assays used for encryption in this study. Shown above are the substrates used and below are the products produced…………………………………………………………………………15

Scheme 3.1 General Scheme depicting the integration of a redox reaction ready by cyclic voltammetry into a symmetrical-key type of encryption……………………………………… 26

Scheme 3.2 A more detailed depiction of the encryption and decryption processes for encryption involving a redox reaction………………………………………………………… 29

Scheme 4.1 ELISA diagram………………………………………………………………… 38

Scheme 4.2 General symmetrical-key cipher scheme with the inclusion of an immunoassay being used to create the encryption and decryption keys…………………………………… 39

Scheme 5.1 Assay for lactate using Lox-HRP……………………………………………… 46

Scheme 5.2 Assay for urea using Urease-GlDH………………………………………….. 47
Scheme 5.3  asymmetrical-key encryption and decryption process .................................. 47
Scheme 5.4  authentication process using asymmetric encrypted signature ....................... 48
Scheme 5.5  key generation scheme using biometric data .................................................. 48
Scheme 5.6  Simplified outline of kRSA message encryption ............................................. 50
Scheme 5.7  Simplified outline of the use of encrypted signatures ..................................... 51
List of Figures

Figure 2.1  HRP with ABTS dye, illustrating data points to encrypt the message………..16
Figure 2.2  HRP with ABTS dye, illustrating data points to decrypt the message………..16
Figure 2.3  The condensed process of encryption and decryption of the message “5, 1, 8”.16
Figure 2.4  Assays used for encryption shown in real time of averages of absorbance (n=5)………………………………………………………………………………………………….17
Figure 2.5  Process used for encryption…………………………………………………….20
Figure 2.6  Decryption process performed by another researcher…………….…….22
Figure 3.1  The use of cyclic voltammetry in order to analyze potassium ferricyanide across certain concentrations in 0.1 M potassium nitrate electrolyte solution. (n=3)………………..32
Figure 3.2  The use of cyclic voltammetry in order to analyze potassium ferricyanide across steps, 4 mM, (n=3)………………………………………………………………………………….32
Figure 3.3  The use of cyclic voltammetry in order to analyze potassium ferricyanide across scan rates, 4 mM, (n=3)…………………………………………………………………………………32
Figure 4.1  ELISA results with secondary antibody dilutions to show variability and consistency (n=3)……………………………………………………………………………….40
Figure 4.2  : ELISA results used for encryption by the message sender. Points chosen for the encryption key are shown as red triangles…………………………………………………….41
Figure 4.3  ELISA results used for decryption by the receiver of the message. Points chosen for the decryption key are shown as green triangles……………………………………………42
Chapter 1. Introduction

1.1 Theory of Bioaffinity-based Assays and Ultraviolet-Visible Spectroscopy

1.1.1 Bioaffinity-Based Assays

The foundation of this dissertation is the use of different biochemical techniques to produce keys to be used in cipher encryption systems. The main techniques used are bioaffinity-based assays, which are commonly used to target certain biological markers. These techniques have three basic parts: the recognition element, the analyte of interest, and a signal transducer. The recognition element consists of a biomolecule which targets a certain analyte. The signal transducer is commonly a redox dye or fluorescent label to create recordable data during an experiment. The research explained in this document utilize enzymes and antibodies as the recognition element and a redox dye as the signal transducer. Assays are recorded spectrophotometrically utilizing an ultraviolet visible (UV-Vis) spectrophotometer.

1.1.2 Enzymatic Assays

Enzymatic assays involve the use of an enzyme as the recognition element. Enzymes are specific to certain analytes which act as the analyte of interest in the assays. Lastly, a redox dye is commonly utilized to produce a colorimetric signal and provides the signal for the assay as the signal transducer. As seen in Scheme 1.1, an enzymatic assay can consist of a single or multiple enzymes to produce a simple, fast assay with a colorimetric response. The substrates that are added in addition to the analyte of interest are present to make
sure the assay proceeds. In the case where there are multiple enzymes in a cascade fashion, such as Scheme 1.1, the first enzyme is related to the detection of the analyte and the final enzyme is related to the signal transducer and the production of the colorimetric result.

1.1.3 Immunoassay

In addition to enzymes, the research in this document utilizes another bioaffinity-based assay involving antibodies as another type of recognition element. The assay performed with antibodies for this research is called enzyme-linked immunosorbent assay (ELISA)\textsuperscript{16–20}. The full version of this assay in the research here uses an antibody that is chemically bound to an enzyme (E) as the recognition element to detect an antigen of interest. The signal transducer is a secondary antibody which has an enzyme bound to it, allowing for the experimenter to perform an enzymatic assay.

The procedure step by step is shown in Scheme 1.2. In this assay, the first antibody (Ab\textsubscript{1}, blue) is added. After washing, the antigen (Ag, red) is added, followed by another wash and the addition of the secondary antibody (Ab\textsubscript{2}, orange). After a final wash, an enzymatic assay is performed just as in 1.1.2 to produce a signal. Immunoassays can also be performed with electrochemistry as well\textsuperscript{21–23}, and are commonly done in clinical environments\textsuperscript{16,24–26}. This process occurs using an antibody’s attraction to a specific antigen. For this to function properly, it is important that both antibodies are specifically attracted to the antigen. Usually both antibodies are the same type of antibody, with one bound to the reporter and the other free.
1.1.4 Ultraviolet Visible Spectrophotometry (UV-Vis)

UV-Vis spectrophotometry is the main instrumentation for a majority of the experiments performed for this document. The technique utilizes a lamp to create white light which is detected after interacting with the sample. This technique can use transmitted, absorbed, fluorescent, or scattered in the data gathering process, depending on the experiment being performed\(^{27,28}\). Transmittance is expressed as a percentage and is the ratio of the light intensity that passes through a sample comparatively to the source light, which is related to absorbance- the measurement of the light that does not pass through. These two values are related by the calculation in Equation 1.1, where A is absorbance and \(\%T\) is the percent transmittance. Fluorescence is where the absorbed light excites a photon in the analyte to a higher energy level, causing the analyte to emit a low energy photon which is then detected. Scattering is where the light is absorbed by the analyte and then released in a different direction with no loss of energy.

Absorbance is used for all the bioaffinity-based experiments herein as it enables calculation of the concentration on the analyte based on the absorbance. Using the Beer-Lambert Law, one can relate the absorbance, A, the molar extinction coefficient-a constant specific to the analyte-\(\varepsilon\), the concentration of the analyte, c, and the optical path length of the sample, l, as seen in Equation 1.2\(^{27,28}\).

\[
A = \varepsilon cl \tag{1.2}\ \\
\text{Beer-Lambert Law}
\]

\[
A = 2\log_{10}(\%T) \tag{1.1}\ \\
\text{Equation 1.1: Absorbance and Transmittance}
\]

The UV-Vis work for the research herein was conducted utilizing a SpectraMax 384 Plus UV-Vis Spectrophotometer\(^{29}\). The light source of this instrument is a xenon flash lamp. The monochromator is used in order to measure the absorbance of samples over a period of time at the
optimal wavelength for each individual analyte, $\lambda_{\text{max}}$. The detector is a photodector, allowing the optical signal to be transduced into electrical signal\textsuperscript{30}. Unless specified, all bioaffinity-based assays were performed with the SpectraMax 384 Plus’s temperature set to 37 °C in 96-well polystyrene microtiter plates.

1.2 Cybersecurity, Ciphers, and Encryption

1.2.1 Background

Privacy, especially the privacy of messages and personal information, has become ever increasingly important in recent times with the advent of computers. Due to the internet, people have had access to people and knowledge they would not have been connected to prior. Unfortunately, this also comes with the trouble that it also opens them up to attacks from those with bad intentions who wish to gain the personal information, messages, and content sent over the internet. Due to this, cryptography, more specifically data encryption, has become an essential part of everyone’s daily life. Cryptography is the study of ‘secret writing’, which is the direct translation of the word from Greek.\textsuperscript{2,3} Cryptography is not new, however, as cryptography has been around since people started sending each other encrypted notes and letters although it was mostly used by lovers, people writing in diaries, wartime communications and people engaging in spy craft. Currently, nearly every computerized function in is encrypted\textsuperscript{1–3}, from the texts, calls, and emails, to every time a person logs into their various accounts, engages in some amount of encryption. As time progresses, encryption systems become increasingly complex and competitive due to the need for more robust and higher security to deal with those who aim to intrude on private messages and personal information.
The current age of cryptography for use by the general population in the computerized era began in the late 1970’s with the announcement of the Data Encryption Standard (DES) by IBM and the NSA. However, this method of encryption only lasted around 20 years until it was cracked in under 56 hours in July 1998 and again in under 24 hours in January 1999 by a non-profit organization, Electronic Frontier Foundation. Setting aside the controversies about the issues that led to the cracking of DES, this is a prime example that newer and better methodologies are needed constantly in the realm of encryption since people are continuously trying to crack the method of encryption, either for personal gain and recognition or for a cash prize. In the research presented here, the aim is to present novel techniques that use different biochemical and chemical methodologies to directly encrypt a message. This is not the first instance of data being used in unconventional ways. Recently, there has been an advance in the multidisciplinary study of unconventional computing. Unconventional computing merges current computer sciences with other professions, such as chemistry, biology, and physics to promote new technologies. This includes encryption being performed with chemical or even biochemical means, as encryption has been used the chemical methods involving fluorescence, photonic crystals, NMR shifts, and molecular computing systems. Also in this field was the integration of biological and biochemical methods using methods involving bacteria, antibodies, and inside of DNA strands. Furthermore, there have been advances in the making of molecular computing systems, molecular logic gates that involved both chemical and biochemical processes for the safekeeping of sensitive information.

1.2.2 Ciphers and Symmetrical-Key Ciphers

The main two methods of encrypting a message are codes and ciphers. Codes consist of replacing one word or phrase with another, such as “Be quiet” becoming “Library” whereas a
cipher is a character for character replacement so that same message of “be quiet” could change to “jdcropdn” considering that a space is in and of itself a character as well. Codes are easily broken by cryptographers and as such are not used, leaving the main focus in modern cryptography fully being the making and breaking of ciphers. As seen in Scheme 1.3, a cipher consists of multiple parts. A cipher encrypts a plaintext (original) message by using an encryption method and an encryption key. Decryption is then performed utilizing the corresponding decryption method and decryption key. As this is symmetrical-key cryptography, both keys are identical.

1.2.3 Asymmetrical-Key Ciphers

Cybersecurity has a second main concern in addition to the protection of data. This second concern is the authentication of the sender of the data, referred to as user authentication. To address these issues, data is encrypted by ciphers or codes and there are encrypted digital signatures to truly show if a person is who they claim to be. As important as message security is, message authentication is considered by many to be more important. This is due to the necessary avoidance of eavesdropping, insertion and deletion attacks on data, and other efforts a bad actor can perform digitally. Different type of cipher, asymmetrical ciphers, can be used for both concerns in cybersecurity. However, asymmetrical ciphers are not to be used for all encryption as they take

Scheme 1.3: A basic symmetrical-key encryption system.
more time compared to their symmetrical counterparts to encrypt and decrypt by the intended parties.

Asymmetrical ciphers between two people use two keys per person, one public and one private for each individual, to send messages. These ciphers allow for two people to securely send messages in public without knowing all the keys involved, even allowing two people who have never met to converse secretly. As cryptographer Bruce Schneier succinctly states, asymmetric encryption “allows you and a friend to shout numbers at each other across a crowded coffeehouse filled with mathematicians so that when you are done, both you and your friend know the same random number, and everyone else in the coffeehouse is completely clueless”\(^1\). This is performed by generating the keys using a mathematical function: integer factorization, modular arithmetic, and exponentiation are primary examples, which is simple to calculate in one direction but much more difficult to reverse engineer. These methods are used in order to create two keys for each individual, a private key for decryption and a public key for encryption, instead of one single key for everything as used in the symmetrical-key cipher systems mentioned earlier. These asymmetrical keys are different from each other and it should not be possible to calculate one from the other. By releasing the public key into the public, anyone who sees that key is then able send a secure message using that key.

As this type of cipher can both be used for encryption and authentication, the proper management of the private and public is paramount. Encryption is done by an outside party to send someone a secure message using the receiver’s public key. For example, if Alice wanted to send Bob a message, she would use Bob’s public key and an encryption method to encrypt the message. Bob would then be able to decrypt the message with his private key and the corresponding decryption method. This method is illustrated in Scheme 1.4.
For the purposes of authentication, Alice would want to use a digital signature to prove that she was the one to send the message to Bob. This is not a signature in the typical sense, as it would not consist of Alice’s name but instead a certain identifier either using a phrase, set of numbers, or some combination of both. To encrypt this signature, Alice would use an asymmetrical cipher to encrypt this identifier with her private key, as seen in Scheme 1.5. Bob would then be able to decrypt the signature using Alice’s public key and the corresponding decryption algorithm. By sending this encrypted signature, Alice is able to authenticate that she was the one to send the message to Bob.

Note: The use of the names “Alice” and “Bob” as communicants is a common practice in cryptography and are only used as placeholders. These names are completely fictional and do not have any connection to a certain individual of individuals.
Chapter 2. Enzyme Encryption


2.1 Introduction

The concepts in the introduction above point to the substantial recent growth of the field of non-traditional computing. This study aims to expand this methodology allowing for the use of bioaffinity-based enzymatic assays, here involving metabolic pathways, for security purposes such as cryptography. These bioaffinity-based assays are the core constructs in the metabolism of all living systems. The assays used in this research use enzymes to transform a specific substrate or substrates into a specific product or products. The method presented here intends to use biochemical assays for encryption by using the outputs to develop a cipher that can be used for information security purposes.

A variation of the Scheme 1.3 shown in the introduction is shown below, adding in the use of the bioaffinity-based assays being performed in this research. In this method of cryptography, the assays are used to create what is known as a key, which is applied to the message along different steps of its travel in order to encrypt or decrypt that message. It is fully necessary for both the encryption and decryption keys to be identical, resulting in the message being transmitted accurately. The produced key is then used to encrypt or decrypt the message using an encryption and decryption method, which are using addition and subtraction in this case, further enforcing the need for the results of the assays to be the same, making the produced keys the same for both the sending and receiving parties.
To this end, it is important to point out the method that the encryption key is used and how the results of the assays can produce that key. In the assays used, the enzyme consumes the substrate or substrates that it is specific to in order to create a product. For these assays it is common for one of the substrates being used to be a dye or for there to be a colorimetric change that would provide a numerical value resulting from the reaction as a function of the reaction progress. The absorbance value responses from the assays used in this method are what is being processed in order to derive the encryption key, which is then used in order to encrypt and decrypt the message, as seen in Scheme 2.1. These values produce the encryption key when the sender performs the assays and the decryption key for the sender when the sender separately performs those assays. This methodology of using an instrument to facilitate a secure encryption method is analogous to what is seen in certain encryption devices, such as the popularized Enigma Machine.

The previously mentioned Enigma Machine uses multiple rotors to encrypt a message. These rotors were responsible for the actual encryption of the message and would only properly decrypt a message if aligned properly. In the research presented here, the instrument used in the
experiment, along with the metabolic, bioaffinity-based assays, work as pseudo-rotors to encrypt a message. Furthermore, just as in the Enigma Machine used rotors in order to encrypt messages by supplying different outputs, the bioaffinity-based assays presented in this work use enzymes at certain parameters of the assays being performed to create different outputs as pseudo-rotors. Enzymes catalyze biochemical reactions of certain chemicals, called substrates, which are specific to those enzymes. During the biochemical reaction of these substrates, the creation of the resulting product or products from these substrates causes a quantitative spectrophotometric change that can be measured using absorbance. The Enigma Machine-like rotors used here are the parameters of the experiment as a whole, including how the instrument is set up, wavelength, buffer pH, and conditions in the assay such as concentrations of substrates and enzymes. Using multiple pre-determined time points along the assays measured in real time was the method used in order in this case to give data values for building the key. This key, resulting from the data acquired from the assays, is then added to the plain text message to be encrypted, which then becomes the cipher text, as seen on the left side of Scheme 2.1. This cipher text is then sent to the receiver of the message who runs the same assays under the same conditions with the same instrument to produce a decryption key. The receiver of the message then subtracts this key from the cipher text to get the plain text message as illustrated on the right side of Scheme 2.1. Both parties also share a separate alphanumeric table that allows for translating letters into numbers, enabling this method to be used. Using multiple wavelengths and multiple assays allows for longer messages to be encrypted in addition to increasing the number of variables used, adding to the security of the method. Looking back at the Enigma machine comparison, the substrate and enzyme concentrations used, and the time points chosen are examples of the rotors that were chosen to be illustrated here. However, it is important to note that it is possible to use a combination of
additional rotors, for example wavelength or temperature, to further solidify the security of this method. As it is important to address the security of this methodology by not repeating the same key, it is important to be aware that the sum of these parameters are able to be changed each time in order the create a new key, strengthening the security. This methodology is similar to the work performed by the Margulies team\textsuperscript{21} insofar as the comparison between their technique and the Enigma Machine, as they created a molecular cipher machine using a synthesized fluorescent molecule which interacted with various chemicals, and was analyzed using a single fluorescent measurement. However, the process described here provides an alternative method utilizing commonly used enzymatic assays, yielding an alternative approach to encryption.

The overall aim of this methodology using biochemical approach would allow for direct encryption of data using bioaffinity-based enzyme assays to create a cipher key. By using well known metabolic enzymatic cascades similar to those mentioned in some of the molecular logic gates and non-conventional computing systems mentioned earlier, these same enzyme systems were dependable in creating a workable cipher for encrypting data. To achieve this, three enzyme assays were chosen: alkaline phosphatase (ALP)\textsuperscript{37-38}, lysozyme\textsuperscript{39-40}, and horseradish peroxidase (HRP)\textsuperscript{41-42}. The advantage of using biochemical methods using enzymes is that they are highly selective and specific for the certain substrates that they consume. Another advantage of enzyme assays is that the results of the assays can be quantified and relatively simple compared to other chemical reactions and methods. Enzymatic assays also can be versatile as well for the purpose of encryption, in that the quantified result will change based on many variables, such as enzyme or substrate concentration, that one can vary in order to heighten security and robustness of the system. By changing these pseudo-Enigma rotor properties such as substrate concentration and enzyme concentration, a multitude of different results can be produced for this method, lowering
the predictability of the results of the assay performed without knowledge of these parameters. Enzymes provide rapid, highly selective reactions to be performed which allows for this process, while not being instantaneous, to be able to be performed quickly with many opportunities for optimization. This optimization allows for this proof-of-concept to be more practical. The process demonstrated here takes 15 minutes in the instrument for the assays to run with minimal preparatory time prior. With different enzymes and different parameters this may be shortened for higher viability and practicality. The nature of performing the experiment in a 96 well microtiter plate as opposed to a cuvette allows for the requisite assays to be performed simultaneously, further reducing the time necessary for analysis. This leaves the limiting factor being the number of wavelengths the instrument is able to concurrently measure.

These enzymatic assays, performed at the same conditions on both the sending and receiving end, will be responsible for building the keys that will be used for encryption and decryption, respectively. By having a set amount of the certain components to these three assays, both the encrypting and decrypting parties would be able to relay an encrypted message. The process demonstrated here as a proof of concept of this methodology used the varying of the concentrations of the substrates for the acquisition of data points for the building of the keys, while keeping the amount of enzyme present constant. Furthering the Enigma comparison, the results here are only looking at changing two major rotors, substrate concentration and time, while keeping the other possible rotors consistent. The output from the bioaffinity-based assays performed was used to create the encrypted message. The output is what is used to create the encryption key, which is then applied to the original text using an encryption method to create a ciphertext. A ciphertext is the transmitted message that is encrypted to protect the message. After the ciphertext is sent, the receiver creates their decryption key by performing the assays using the
same parameters that were used to create the encryption key. This decryption key is then used in the decryption method in order to produce the original plaintext, receiving the message as intended that was transmitted in a way that it could not be read or altered by an intruder. This process follows Kerchoffs’ Principle, a rule used in cryptography that states that in order for a cipher system to be secure, that only the keys need to be secret, and that it is not essential for anything else to be secret. To follow this, the keys, and by extension the assay parameters, are only to be known by the sender and receiver but the methodology is public.

2.2 Materials and Methods

2.2.1 Chemicals

Alkaline phosphatase (E.C. 3.1.3.1), lysozyme (E.C. 3.2.1.17), horseradish peroxidase (E.C. 1.11.1.7), p-nitrophenylphosphate (pNPP), 3,3’,5,5’-tetramethylbenzidine (TMB), hydrogen peroxide, micrococcus lysodeikticus cells, sodium carbonate, and sodium bicarbonate were all purchased from Sigma-Aldrich. Hydrochloric acid was purchased from EMD Millipore. An ELGA PURELAB flex water purification system was used to obtain ultrapure (18.2 MΩ·cm) water for each experiment.

2.2.2 Enzymatic Assays

The enzymes used for the assays for encryption and decryption are alkaline phosphatase (E.C. 3.1.3.1), lysozyme (E.C. 3.2.1.17), and horseradish peroxidase (E.C. 1.11.1.7).

Alkaline phosphatase (ALP) dephosphorylates p-nitrophenylphosphate (pNPP) into p-nitrophenol (pNP), which results in a yellow color that is observed at $\lambda=405$ nm.$^{38,43}$
Lysozyme breaks down two residues, N-acetylmuramic acid and 2-acetylamino-2-deoxy-D-glucose, found in the cell walls of gram-positive bacteria, resulting in the lowering of the structure and integrity of the cell walls\textsuperscript{44}. The breaking down of the cell’s walls can be spectrophotometrically observed at $\lambda=450$ nm\textsuperscript{40,45}, as a decrease of absorption as time passes.

Horseradish peroxidase (HRP) reduces hydrogen peroxide into water while oxidizing a dye which is read on the spectrophotometer. An assay with HRP is able to be performed with multiple different dyes, however, the one chosen in this case was 3,3’,5,5’-tetramethylbenzidine, which absorbs at $\lambda=650$ nm\textsuperscript{42,46} for its first oxidation state.

These three assays can be seen in Scheme 2.2, with specifically focusing on how this approach is utilizing enzyme assays to build the encryption key. Seen in this figure is a section of Scheme 2.1, which shows the three enzymes being used in the method presented here.

2.2.3 Cipher

The process of encryption and decryption follows the following process illustrated with one enzyme system here to prove proof of concept. Using HRP with a different dye, ABTS, the encryption of the area code of Albany, NY, “518” is shown. This dye is different than the HRP assay used in the full encryption system in section 3.0 and 3.1. This is due to the fact that ABTS
is measured at 405 nm, which would interfere with the ALP assay if the full assay system were performed at the same time. First, the assay is performed at the pre-determined settings that will be used by both the sending and receiving parties.

The absorbance readings at a certain wavelength as seen in Figure 2.1 are 1.6, 2.3 and 3.1, respectively. These data values are rounded to the nearest whole number and then added to the message so “5, 1, 8” becomes “7, 3, 11”. This addition was used in a similar manuscript\textsuperscript{21}, as it illustrates a straightforward methodology of showing the viability of the method to be applicable for encryption, without taking away from the base methodology used in order to create the encryption and decryption keys. This encrypted message “7, 3, 11” is then sent to the receiver, who then repeats the same experiment, with the same parameters. The data points taken from the certain time points seen in Figure 2.2 provided values of 1.6, 2.3, and 3.1, which were rounded and then used by the sender, who subtracted the points from the message, leading “7, 3, 11” to be correctly decrypted to be “5, 1, 8”, the original message. The outline of this process is seen in Figure 2.3. This demonstrates it is possible to use this technique to encrypt and decrypt a message correctly, albeit with a simple message. Furthermore, by changing parameters the resulting key will change each time, allowing one to change parameters to create different keys as

\[ \begin{align*}
5 & \quad \text{Encryption} \\
1 & \quad \text{Encryption} \\
8 & \quad \text{Encryption}
\end{align*} \]
explained previously. This can be done by changing many or even by changing a single parameter. For example, by doing this above assay keeping all other parameters the same and using half of amount of enzyme present, the data values then become 0.9, 1.21, and 1.7, making the “5, 1, 8” message be encrypted to “6, 2, 10” due to the change in the encryption key.

2.3 Results and Discussion

2.3.1 Reproducibility and variation check

To make sure that the method presented here is a reliable process for the encrypting and decrypting of messages, it is completely essential that the assays used are reproducible. The three assays were analyzed at different concentrations of substrates to prove their precision as illustrated in Figure 2.4A-C. As these enzymes behave differently for the parameters chosen, the time values of each of the figures below are not the same. However, it is important to note that the important part for this technique is not for all of them to behave similarly, but to be consistent internally within multiple runs for accurate encryption and decryption.
2.3.2 Encryption

This method will now be used to encrypt a short message of “LOOK OUT”. In order to do this, the process seen in the encryption previously is seen with one extra step involving the changing of alphanumerical text into purely numerical text to use addition/subtraction. The first step is to convert the original message from letters into numbers using a public alphanumeric cipher (Table 2.1). The ranges in this table below are based off of a multiplicate, 4x, of the highest standard deviation between the trials in the parameters shown above using the three assays. This step is important as it allows for the encryption method to be used since it is number-based due to the numerical results of the assays. The numbers chosen for each character of the message correspond to the average value from the range in the alphanumerical cipher table as shown in Table 2.2. The public alphanumerical table should be created based off of the relative reproducibility of the assays used for the encryption/decryption process, specifically the highest standard deviation resulting from the three assays performed. This alphanumerical cipher does not need to be kept secret due to the rest of the encryption process being the secure method of encryption. This alphanumerical cipher would be considered ‘public’ as it is not important to keep the keys secret. This process of secrecy of the keys, the keys that will be produced by the enzyme assays for this method, follows Kerckhoffs’ Principle which states that the keys need to be the only secret part of a cipher system.
for it to be secure\(^1\). Another important factor in the security of an encryption process is key length. Here, for simplicity, is a key that matches in length to the message being sent. The key length in this methodology is primarily dependent on the number of data points in the experiments being performed. By using a higher sampling rate, such as using every 10 seconds or 15 seconds rather than the 30 seconds mentioned here, the result would be the potential for longer keys without compromising the integrity of the system by repeating the key within the same message.

Once the alphanumerical table is used in order to convert the original message to a numerical message, the three assays are performed (Figure 2.5A-C) using a pre-determined set of parameters. These parameters are, in this case, the pseudo-Enigma-Machine rotors mentioned previously. These parameters include, but are not limited to, enzyme and substrate concentration, wavelength, time points chosen, and buffer pH. These parameters must be known to both the sending and receiving parties, ideally using a different set of parameters for each message sent for increased security. An example of a set of parameters for this method can be seen in Table 2.3. The parameters used in the encryption process below are similar to the parameters of the assays performed above, however, they do not match the parameters used for the experiments performed in Figure 2.4. This modification of some of the parameters was performed in order show the quantitative nature of this methodology and to illustrate that this method is not only applicable at the nine sets of experimental parameters shown in Figure 2.4.

As the keys need to be secure and the assays which are being performed, along with all of the parameters mentioned, both parties would need to have a secure manual of pre-determined

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>pH</td>
<td>7.2</td>
</tr>
<tr>
<td>Temperature</td>
<td>37 °C</td>
</tr>
<tr>
<td>Enzymes</td>
<td>Lysozyme, Horseradish Peroxidase, Alkaline Phosphatase</td>
</tr>
<tr>
<td>Wavelength(s)</td>
<td>450, 650, 405</td>
</tr>
<tr>
<td>Substrate concentrations</td>
<td>10 mM all</td>
</tr>
<tr>
<td>Enzyme Units</td>
<td>5 mU all</td>
</tr>
<tr>
<td>Time points for key</td>
<td>Lys 300s, HRP 125s, ALP 500s, HRP 760s, Lys 900s,…</td>
</tr>
</tbody>
</table>
parameters for each key they would be making. As the key length would be determined here, it would be important to choose a large number of time points so that longer messages may be used as well as short messages. This step in this process, the part where both parties need to have the same set parameters for this specific message, is the least secure step in a cipher since it is the most vulnerable during transport between the parties. This would overall be done in an analogous process to historical devices\(^1\)\(^2\), such as the Enigma Machine and other common cipher systems, where both parties had a manual or book of listed parameters and would have some reference as to which they need to use for a particular message.

For the next step, in which the encryption key is produced using certain times chosen in each assay to correspond to the output which is responsible for that part of the key. These chosen time points would be a part of the pseudo-Enigma rotors parameters that would be pre-determined
for each encrypted message, changing for each one. Since the message demonstrated here has eight characters in it, eight time points are chosen across the three assays (Figure 2.5D). To make sure both parties choose the same time points, those times would be listed along with the assay parameters that was given to both parties. With this derived key, the encryption method is then used to change the plaintext into a secure ciphertext (Figure 2.5E). For this method, a simple addition is used so the keys corresponding to each number from the original text is added to that original text. It should be noted that although addition/subtraction and only 8 points were chosen in this particular message, an assortment of other parameters could be used in order to heighten the security of this process. Addition/subtraction was used in order to focus on the use of enzymatic assays to encrypt a message as a basic principle, allowing for more focus to be on the methodology of creating the symmetrical keys as opposed to the encryption method itself. By using a more secure algorithm and by choosing a larger number of points to build a key, the process would be more secure. As this is a proof-of-concept, addition and subtraction were used in order to open the door to use such techniques in further experimentation. By just using addition/subtraction this would be open to a brute-force attack similarly to many other commonly used ciphers throughout time, including the Data Encryption Standard that was mentioned earlier, which could be alleviated by combining this technique with a more secure algorithm or using a longer key that does not match the number of characters in the message.

The text that is created is the encrypted ciphertext, which is then sent to the receiver. In this case the text that would be sent would be: “5.61, 2.39, 2.58, 5.67, 7.31, 2.62, 3.55, 1.31”. Since this is encrypted, it would be directly translated as “CPPC1AFY” according to Table 2.1, without any decryption. These encryption steps were performed by the first author, who then sent the ciphertext over email to the second author.
2.3.3 Decryption

Once the ciphertext was sent over email to a second lab member, this second person acted as the receiver and proceeded to decrypt the message. This process consists of the four steps above in a near-reverse order. This process is illustrated in Figure 2.6. The receiver first performs the assays at the same pre-determined parameters that were used by the sender (Figure 2.6A-C). Also using the same parameters as the sender, the received uses the same time points for the three assays to build their decryption key (Figure 2.6D). This decryption key is then subtracted from the received message (Figure 2.6E). This now leaves the deciphered message that needs to be transformed back into the original characters using the same public alphanumeric table that was used by the sender (Figure 2.6F). That leaves the original message, which here is seen to be correctly received and accurately interpreted to be “LOOK OUT”.

Figure 2.6: Decryption process performed by another researcher. A reverse of the encryption process was used, starting with the same three assays from Figure 2.5A-C being performed in 2.6A-C. The same time points as encryption were used to find data for the purpose of creating a decryption key (2.6D). This decryption key was than subtracted from the ciphertext sent to the receiver, seen in 2.6E, to produce the original message. This is then transformed back into text in 2.6F using the alphanumeric Table 2.1, correctly showing the message as “LOOK OUT”.

Once the ciphertext was sent over email to a second lab member, this second person acted as the receiver and proceeded to decrypt the message. This process consists of the four steps above in a near-reverse order. This process is illustrated in Figure 2.6. The receiver first performs the assays at the same pre-determined parameters that were used by the sender (Figure 2.6A-C). Also using the same parameters as the sender, the received uses the same time points for the three assays to build their decryption key (Figure 2.6D). This decryption key is then subtracted from the received message (Figure 2.6E). This now leaves the deciphered message that needs to be transformed back into the original characters using the same public alphanumeric table that was used by the sender (Figure 2.6F). That leaves the original message, which here is seen to be correctly received and accurately interpreted to be “LOOK OUT”.

<table>
<thead>
<tr>
<th>Decryption Key</th>
<th>Ciphertext</th>
<th>Assay (#)</th>
<th>D. Key (subtraction)</th>
<th>Plaintext</th>
</tr>
</thead>
<tbody>
<tr>
<td>1(L) 0.8002</td>
<td>5.61 ALP 1</td>
<td>0.8002</td>
<td>4.81</td>
<td></td>
</tr>
<tr>
<td>2(O) 0.1760</td>
<td>2.39 Lysozyme 2</td>
<td>0.1760</td>
<td>2.21</td>
<td></td>
</tr>
<tr>
<td>3(O) 0.3674</td>
<td>2.58 HRP 3</td>
<td>0.3674</td>
<td>2.21</td>
<td></td>
</tr>
<tr>
<td>4(K) 1.2209</td>
<td>5.67 ALP 4</td>
<td>1.2209</td>
<td>4.45</td>
<td></td>
</tr>
<tr>
<td>5(space) 0.1615</td>
<td>7.31 Lysozyme 5</td>
<td>0.1615</td>
<td>7.15</td>
<td></td>
</tr>
<tr>
<td>6(O) 0.4315</td>
<td>2.62 HRP 6</td>
<td>0.4315</td>
<td>2.19</td>
<td></td>
</tr>
<tr>
<td>7(U) 1.8588</td>
<td>3.55 ALP 7</td>
<td>1.8588</td>
<td>1.69</td>
<td></td>
</tr>
<tr>
<td>8(T) 0.1465</td>
<td>1.31 Lysozyme 8</td>
<td>0.1465</td>
<td>1.16</td>
<td></td>
</tr>
</tbody>
</table>

| Decrypted Message | |
|-------------------||
| 4.81 L | 2.21 O |
| 2.19 O | 4.45 K |
| 7.15 Space | 1.69 U |
| 1.16 T | 
2.4 Conclusion

In this day and age, with the need for the secure sending of messages in a digital world, different techniques of encrypting data need to be researched and utilized. The proof of concept research presented here illustrates the first method that uses bioaffinity-based enzymatic assays, a highly specific yet flexible medium, for the purposes of creating encryption and decryption keys for encrypting and decrypting messages via a symmetrical-key cipher. These biocatalytic reactions allow for many cipher keys to be able to be produced by changing the parameters used in the enzyme assays, such as substrate concentration which was used here or multiple other facets including, but not limited to, enzyme concentration, buffer pH, and wavelength. These parameters, along with the pre-determined time points chosen in order to build the encryption/decryption key not only allow for the number of available keys to be exceptionally large, but also fortifies the security of the technique since one does not want to repeat the same set of parameters twice, in order to reinforce the security of the encryption method from outside attacks. In addition, there are a vast number of enzymes currently used commonly for various assays in point-of-care diagnostics and for other methodologies, allowing for a more complex system as the three enzymes mentioned here are not the only three possible. As seen in many of these assays, the signal is able to be amplified as well, showing another possible rotor for this method. There have also been advancements of those who have produced genetically modified and synthetic enzymes, further expanding on the possibilities of potential keys that may be produced using this methodology.

This methodology was proven to be an applicable approach to encryption and decryption with the process outlined here. The fact that a transmitted message was able to be correctly decrypted using bioaffinity-based assays yields to biocatalytic reactions being a viable technique
to use for the purpose of encrypting messages. This being performed by two separate people in the research laboratory further confirms the viability of this method. Ideally, this could be used with a cellphone camera since all the assays are able to be analyzed by using visible light, which can be quantified in a cellphone’s camera. This method can be used in a wide range of applications throughout the cryptographic community, and other security applications in a lay setting due to the ease of methodology and the substantial number of variables applicable to such a method.
3. Cyclic Voltammetry Encryption

Adapted in part with permission from McGoldrick, L. K., Halámek, J. “Encryption and Decryption with Symmetrical Keys Utilizing Redox Reaction via Advanced Encryption Standard” Manuscript in Preparation.

3.1 Introduction

The novel methodology described here is designed for building encryption and decryption keys in symmetrical-key cryptography. This approach provides a viable alternative to the currently used cryptographic processes utilizing computerized random number generators. To this end, encryption and decryption keys were developed utilizing a chemical redox reaction analyzed by an electrochemical technique. Electrochemistry provides a powerful, consistent parallel to the currently used methods and has ease of use as some instruments, such as the one used for this research, have BlueTooth® capabilities. In order to show that this method is a viable alternative in the current realm of data security, the current standard established for encryption, the Advanced Encryption Standard (AES), was used in order to encrypt and decrypt a sample message. This message was encrypted using 128-bit cryptographic keys produced from the electrochemical analysis of the chemical oxidation/reduction reaction. This methodology shows that by using a set of parameters for an electrochemical redox experiment that are consistent between the sender and receiver of a message, a message can be encrypted, securely sent, and subsequently decrypted. The innovative process outlined here uses a vast number of parameters which may be changed in order to create a multitude of keys, providing intrinsic security for the technique. This methodology not only shows that electrochemical experimentation for encryption is able to produce a multitude of unique keys by changing the parameters chosen for each new key, but this method is also a viable means for producing keys to be used by the current standard, the Advanced Encryption Standard.
The method proposed here is used in the building of a cipher to encrypt a message using a redox reaction combined with cyclic voltammetry. The results of a redox reaction explained below will be used in the building of the encryption key, which is then used in the encryption method to change the plaintext in the encrypted ciphertext that will be sent to the other party. This receiving party will perform the same experiment under the same parameters to produce the same data values as the encryption key for their decryption key in order to properly decrypt the message. The method of encryption can be changed depending on the level of security necessary for the message being sent. The encryption method can be DES or its successor, Advanced Encryption Standard (AES)\textsuperscript{2,3} for higher security but could also be more common mathematical function such as addition/subtraction or the XOR function for lower security needs.

In order for the novel methodology outlined here to be interfaced into the currently used symmetrical-key encryption processes, it is highly necessary for the encryption and decryption keys to be the same. Due to this restriction, it is completely mandatory for the method of acquiring

---

**Scheme 3.1:** General Scheme depicting the integration of a redox reaction ready by cyclic voltammetry into a symmetrical-key type of encryption\textsuperscript{1}
the experimental data to be highly consistent between runs, so that if both the receiver and sender of the message perform the same experiment, they receive similar enough data in order for the subsequent decrypted message to not result in nonsense. This leads to the fact that both parties need to have a pre-determined set of parameters, including, but not limited to, concentration of the materials used, the buffer used, potential points chosen for current readings to build key and the parameters for the cyclic voltammetry scan itself such as potential range, step, scan rate, and others. The acquisition and distribution of a ‘ledger’ of sorts containing all of this information is the most insecure part of this encryption method, which is the same problem with any symmetrical cipher technique. This is due to Kerckhoffs’ Principle, which states that in order for a cipher system to be secure, only the keys need to be secret, and that it is not necessary to keep the rest of the method secret since it should be secure even if known by an outside party\textsuperscript{2,3}. Hence, another name of this type of cryptography is “secret key cryptography”\textsuperscript{2,3}. Since the redox reaction monitored by cyclic voltammetry is the building block of the key, it is necessary for those sets of parameters to remain secret, but the encryption method need not be. It is also important to have more than one set of parameters due to the more information an outside cryptanalyst has, the more likely they would be able to crack the encryption. As such, by changing the parameters every time, the key will be changed which will result in the encrypted messages being different, even if they contain the same words or phrases. This will hinder a third party even if they have received previous encrypted messages.
3.2 Materials and Methods

3.2.1 Chemicals

A PalmSens EmStat Blue (Houten, The Netherlands) was used for all data collecting in conjunction with PalmSens’s PSTrace4 Software (Houten, The Netherlands). The reversible redox reaction that was used consisted of ferricyanide to ferrocyanide and the reverse, which consists of the gain and loss of one electron \(^{67}\) as seen in Equations 3.1 and 3.2. This reaction was measured in a 0.1 M potassium nitrate electrolyte solution and measured at various levels of concentration, step, and scan rate. Potassium nitrate and potassium ferricyanide were acquired through Sigma-Aldrich (St. Louis, MO, USA). For the analysis, platinum electrodes were used as working and counter electrodes with an Ag/AgCl reference electrode. The electrodes were products of CH Instruments, Inc. (Austin, Texas, USA) with the platinum electrode having the part number CHI102 and the reference Ag/AgCl having the part number CHI111.

\[
Fe^{III}(CN)_6^{3-} + e^{-} \rightarrow Fe^{II}(CN)_6^{4-}
\]
Equation 3.1: reduction reaction of ferricyanide to ferrocyanide

\[
Fe^{II}(CN)_6^{4-} \xrightarrow{ox} Fe^{III}(CN)_6^{3-} + e^{-}
\]
Equation 3.2: oxidation reaction of ferrocyanide to ferricyanide

3.2.2 CV Parameters

As stated above, this reaction was measured in a 0.1 M potassium nitrate electrolyte solution and measured at various levels of concentration, step, and scan rate. The concentration variants were 2, 4, 6, 8, and 10 mM solutions of potassium ferricyanide. The step was varied by using 2, 3, 5, 10, and 50 mV steps using the 4 mM potassium ferricyanide sample. Scan rate had different rates of 20, 50, 100, 150, and 200 mV/s. Scans were performed between -0.2 V and 0.9 V.
In order to prove that this method is reliable for producing a robust key to use for encryption, the results will be used in the current standard for encryption today, Advanced Encryption Standard (AES)\textsuperscript{1–3}. Scheme 3.2 shows the encryption and decryption processes. AES requires a key of 128, 192 or 256 bits (or 16, 24, or 32 bytes, respectively). To use this, the first step is to transfer the data, which is currently in ‘text’ form into bytes. In this case, a simple method of doing this is relating the chosen data points into their corresponding hexadecimal (hex) bytes. Each text number produces a pair of digits in hex, which accounts for a single byte. However, the selection of data points would need to have 16, 24, or 32 text digits total in order to use this method. As this is a proof of concept, the lowest requirement, 128-bit (or 16 bytes), will be used, which requires a total of 16 text digits from the data used in the cyclic voltammetry scan. To this extent, the data was rounded to the nearest whole number and that number was then used. If the value would result in a single digit number, a zero would be used prior for consistency and ease of access: “9” becoming “09”. The low average standard deviation between each of these experiments seen below for concentration, step, and scan rate, allow the use of this methodology in utilizing whole numbers for the building of the cryptographic keys.
By choosing a select amount of data points from the experiment, a sender and receiver can use these data points in their separate experiments to encrypt and decrypt a select message, respectively. Since this method is highly precise due to the nature of the experiment performed, two people separately performing the experiment should achieve the same results and be able to translate a message properly. Also aiding in this methodology is the variance between parameters, so, as long as a third party does not know the exact parameters that are performed to encrypt and decrypt a particular message, it would be very difficult for them to correctly decrypt the message. This leads to one necessary preparatory step to this methodology. This is due to both parties needing to use the same parameters for a particular message, requiring them both to have prior knowledge of the particular set of parameters before the message is sent. For example, both the sender and receiver would have a “ledger” of all of the parameters they could potentially use. With the encrypted message, the sender would also send an unencrypted section which would tell the receiver which set of parameters they chose, “page 42” for instance. This is the least secure step of this method of encrypting a message, since the receiver needs to have this “book of codes” in their possession and have received it in the first place, both of which would be the ‘weak links’ in this process. This is due to the fact that a third party could steal it from them, steal it in transit, or just copy the contents, although they would still need the equipment and knowledge in order to perform the experiment correctly.
3.3 Results and Discussion

3.3.1 Reproducibility and variation check

To show that this novel application of electrochemistry to encryption would be a viable technique to use, the commonly used electrochemical conversion of ferricyanide/ferrocyanide as the redox species was used due to it being a well understood reaction for cyclic voltammetry analysis. As this molecule is not the only possible redox species for such an experiment, the chemical used would be yet another parameter that can be changed for security purposes. Due to the nature of the encryption being done, the keys produced need to be identical. Due to this, the reproducibility of this method must be tested. To visualize this, multiple different tests were performed observing the ferricyanide-ferrocyanide redox reaction by cyclic voltammetry. As one of the facets of this methodology include being able to change parameters to produce different keys, multiple parameters were tested. The main three parameters that were tested were concentration of the ferricyanide, the scan rate of the cyclic voltammetry scan, and the step of the cyclic voltammetry scan. These are not the only parameters that may be changed for one encryption/decryption key to the next, others may be changed as well in order to heighten the security of the method.

As seen in Figure 3.1, the effect of concentration creates an increase in the resulting current of the system as expected. The results are consistent throughout the tests ranging from 2 mM to 10 mM solutions of potassium ferricyanide. In Figures 3.2 and 3.3, scan rate and changing the step used are also being observed, respectively. Both of

![Figure 3.1: The use of cyclic voltammetry in order to analyze potassium ferricyanide across certain concentrations in 0.1 M potassium nitrate electrolyte solution. (n=3)](image-url)
these were performed using the 4 mM solution. It is seen that these three effects all have a profound change on the results of the system. More importantly, the deviation between scans of the same parameters for all three are all low. This makes cyclic voltammetry viable for this method since it is a reliably consistent method and changing the parameters causes a tangible difference in the output of the result. This allows the method to be viable as the correct key will only be created by using the correct set of parameters and there would be barely any overlap between sets of parameters.

3.3.2 **Encryption and Decryption**

Due to the nature of the results being two-digit numbers, eight data points are necessary or a fewer number of points can be chosen and repeated. The values of runs done at four potential values were chosen from the cyclic voltammetry scan and are repeated twice. This effectively denotes a set of parameters where the potential values are chosen twice, this is not always necessary but was used in this example as it could be a possibility for a set of parameters for use in this method. Table 3.1 shows the values that were chosen and the corresponding hex that relates to the data points. These points are then compiled and repeated, resulting in a key of

![Graph 3.2: The use of cyclic voltammetry in order to analyze potassium ferricyanide across steps, 4 mM, (n=3)](image)

![Graph 3.3: The use of cyclic voltammetry in order to analyze potassium ferricyanide across scan rates, 4 mM, (n=3)](image)

**Table 3.1: Current at select potentials that is to be used to create the encryption key.**

<table>
<thead>
<tr>
<th>Potential (V)</th>
<th>Current (mA)</th>
<th>Current in hex</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.270731</td>
<td>21</td>
<td>32 31</td>
</tr>
<tr>
<td>0.315703</td>
<td>25</td>
<td>32 35</td>
</tr>
<tr>
<td>0.396652</td>
<td>19</td>
<td>31 39</td>
</tr>
<tr>
<td>0.516577</td>
<td>12</td>
<td>31 32</td>
</tr>
</tbody>
</table>
“32313235313931323231323531393132”, as the 16 byte encryption key to use in AES. This key, along with the message that needs to be sent: “it’s dangerous to go alone, take this” will now be put through the encryption method, AES, in order to produce the ciphertext of this message. Due to the online calculator used in order to process the encryption and decryption using AES, the message also needs to be translated into hex. Once the key is applied through AES to encrypt the message, the ciphertext is produced. Since this ciphertext is encrypted, it is the message that is sent to the receiver. Directly translated from hex to text, the ciphertext is complete nonsense, reinforcing that a third party who intercepted the message could not read it without knowing the key. The ciphertext would be directly transcribed to be “т5Д,†УѣІ%ѳЦја/і&JŎ+SMм Mỹɓ»Ĕ„я&ŎМ””. The receiver then uses the same potential values at the same instrument and experiment parameters to formulate their own key, producing the decryption key. The sent ciphertext is then decrypted through AES and then translated back into text from hex. The ciphertext was correctly translated as “It’s dangerous to go alone, take this”. This process is seen in Table 3.2, through the encryption and decryption process using AES. As stated in the table regarding the extra 0’s at the end of the decrypted message in hex, the program needs to fill text in order for it to be a certain length, so these 0’s are “padding” to standardize the length of the message.

### 3.4 Conclusion

This research provides proof-of-concept for a novel approach utilizing a redox reaction-based technique in order to build a robust cipher system for the encryption of messages. In the

<table>
<thead>
<tr>
<th>Table 3.2: Encryption and decryption process steps through AES.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Message</strong></td>
</tr>
<tr>
<td><strong>Message (hex)</strong></td>
</tr>
<tr>
<td><strong>Encryption Key</strong></td>
</tr>
<tr>
<td><strong>Ciphertext</strong></td>
</tr>
<tr>
<td><strong>Decryption Key</strong></td>
</tr>
<tr>
<td><strong>Decrypted message (hex)</strong></td>
</tr>
<tr>
<td><strong>Decrypted message</strong></td>
</tr>
</tbody>
</table>
research presented, a cyclic voltammetry experiment using the ferricyanide/ferrocyanide redox reaction was used in order to create encryption and decryption keys that are used in the encryption of data, in this case a message. As with similar symmetrical-key cryptography techniques, this requires both the sender and receiver to produce the same exact key and it was proved that the results of the experiment are consistent enough to be applicable for this methodology. Both sender and receiver of the message would need to have foreknowledge of the instrumental and experimental parameters for each message sent and to be able to have enough sets of parameters to last themselves a moderate amount of time, a “book of cipher parameters” in other words. This is due to the fact that the repeated utilization of the same key is a deterrent to the security of the process, which has been seen as many encryptions have been ‘broken’ over the years due to careless actions such as reusing an old encryption key. By having this methodology be applicable to be used with the current standard for encryption, AES, it demonstrates that it is possible to use experimental results of an electrochemical experiment to build a secret key in order encrypt data and successfully decrypt it using a current high-end cryptographic algorithm. As this methodology concerns the derivation of a key and does not interfere with the actual encryption method it is viable for any symmetrical-key cipher method, either ones currently used or ones that will be developed in the future. With more points being used, the security of this method would be enhanced from using a 192 or even 256 bit key compared to the 128 bit key successfully used here, at the expense of speed, both in analysis and the use of the AES algorithm itself. This process is also able to be broadly used as there are electrochemical devices, including the one used in this experiment, which may be used in conjunction with a cell phone using either a direct attachment or BlueTooth® technology, reducing the need for a laboratory environment for such a technique. This is due to the fact that the process outlined here in this research utilizes an electrochemical
device that has Bluetooth® capabilities, further enabling the applicability of this method for rapid use with current technologies
4. Immunoassay Encryption

Adapted in part with permission from McGoldrick, L. K., Halámek, J. “AES Encryption Utilizing Cryptographic Keys Derived from Immunoassay”. Manuscript in Preparation

4.1 Introduction

For our previous manuscript, the methodology focused on using enzymatic assays in order to encrypt data with an addition/subtraction encryption/decryption method. This very basic encryption technique allowed for another biomolecule to be used for encryption in addition to the commonly seen DNA methods mentioned previously. As opposed to the enzyme-substrate interactions we used before, immunoassays rely on the use of antibody-antigen recognition between the paratope of the antibody and the epitope of a specific antigen. In addition, the detection method in an immunoassay can have multiple types of labels, and the system presented for the process outlined here utilizing an enzyme bound to the secondary antibody is not the only detection method for an immunoassay. The approach listed here uses another type of bioaffinity-based interaction, antibody-antigen based immunoassays, in addition to the current standard of encryption, AES. AES is a complex mathematical algorithm which is used as the current standard for normal and high level encryption and is currently used in most forms of communication. The approach presented here is beneficial as it shows the applicability of such a system in the current cryptographic environment while also introducing an additional affinity interaction to this current approach of utilizing biomolecules for cryptographic purposes.

This research presents a combination of an immunoassay methodology, specifically an enzyme-linked immunosorbent assay (ELISA), with the algorithm, which is the current high standard in cryptography, the Advanced Encryption Standard (AES). By using the data gained from this immunoassay, one can create a cipher key. By both the encrypting and decrypting parties
using the same set of parameters for a particular message, their keys should be symmetrical. This approach is a focus on providing cryptographic keys by nonconventional means, which heightens the security of the method as there are a large amount of variables in an ELISA experiment itself, yet alone in how one could choose the data points in order to build the key. However, and just as importantly, immunoassays are known for their consistency, selectivity, and sensitivity\textsuperscript{76,78}, which are all important facets for use as a methodology in order to produce cryptographic keys. The only hardship for the method, which is a similar problem for all symmetrical-key approaches, is that both parties would need a list of experimental parameters for each message to be securely sent, as these provide the keys so they should be secret as well. Each message should also have its own set of parameters, as ciphers are progressively easier to break if the same keys are used multiple times\textsuperscript{1–3}. As such, both the sender and receiver would need a ledger of parameters that would be available for all of their messages.

**4.2 Materials and Methods**

**4.2.1 Chemicals**

A SpectraMax 384 Plus spectrophotometer was used for all measurements. The immunoassay experiment used AffiniPure donkey anti-human IgG and AffiniPure donkey anti-human IgG conjugated to horseradish peroxidase (HRP, E.C. 1.11.1.7), both from Jackson ImmunoResearch Inc. (West Grove, PA) as the primary and secondary antibodies, respectively. Human Gamma Globulin (HgG) was used as the antigen, also from Jackson ImmunoResearch. The following reagents were purchased from Sigma-Aldrich (St. Louis, MO): hydrogen peroxide, 2,2’-azino-bis(3-ethylbenzothiazoline-6-sulfonic acid) (ABTS), bovine serum albumin (BSA), sodium chloride, potassium chloride, sodium phosphate dibasic, and potassium phosphate monobasic anhydrous, TWEEN\textsuperscript{®} 20, sodium citrate and citric acid. An ELGA water purification
system, the PURELAB flex, was used to obtain ultrapure (18.2 MΩ·cm) water for the buffers. The AES algorithm was performed using Cryptomathic’s online AES calculator\textsuperscript{85}.

1.2.2 Immunoassay

The bioaffinity-based assay performed in this research is an example of a full sandwich Enzyme-Linked Immunosorbent Assay (ELISA)\textsuperscript{16}. ELISA has been combined with different techniques in multiple fields such as electrochemistry\textsuperscript{21,23,79,86,87}, bioelectronics\textsuperscript{22,88}, clinical services\textsuperscript{89,90} and even one for very basic encryption\textsuperscript{56}. A full sandwich ELISA assay consists of 4 main parts: a primary antibody (Ab\textsubscript{1}), a secondary antibody (Ab\textsubscript{2}), an antigen, and a reporter which is usually located on the secondary antibody. Scheme 4.1 demonstrates how these components align. In the process demonstrated here, the reporter consists of an enzyme (E) bound to the secondary antibody, which is used similarly to other techniques presented in this document in producing a colorimetric response. For this research Ab\textsubscript{1} and Ab\textsubscript{2} were the same antibody except for Ab\textsubscript{2} was bound to HRP. The primary Ab\textsubscript{1} was bound to the well plate being used for the experiment. After washing, a specific antigen that both Ab\textsubscript{1} and Ab\textsubscript{2} target is added. After washing an enzymatic assay for HRP is performed producing a colorimetric result.

4.2.3 Cipher

A very general scheme of encryption is as follows: the original text (also called plaintext) is processed through an encryption method, which is commonly combined with an encryption key, to produce the encrypted text (or ciphertext). Here, the data from an immunoassay experiment is being used to produce the encryption and decryption keys. Decryption is the reverse, where the
ciphertext is put through the corresponding decryption method with a decryption key, which results in the original plaintext. This can be seen in the diagram in Scheme 4.2 with the application of the immunoassay outlined in this research.

This cipher scheme is known as symmetrical-key encryption\textsuperscript{1–3} due to both parties needing the encryption and decryption keys to consist of the same exact values. An important note about cryptography is that the keys are what is needed to be kept secret, the encryption method is usually publicly accessible. This follows Kerckhoffs’ Principle, which broadly states that the system should be secure if a third party has access to all of the parts involved minus the key\textsuperscript{1–3}. This principle is implied still today, which forces pressure into the quality of the secret keys being used for cipher systems. The encryption method, however, is not bound to the same secrecy, in fact it is even better for the method to be public so it may be tested. This method can be basic mathematical functions, for example addition/subtraction\textsuperscript{75} or XOR, or a complex algorithm, for example the Data Encryption Standard (DES) or its successor Advanced Encryption Standard (AES) seen here. The method used depends on the level of encryption needed, with higher security systems sacrificing an amount of processing time for higher security.
4.3 Results and Discussion

4.3.1 Reproducibility and variation check

The research described here involves applying a commonly used type of immunoassay, full sandwich ELISA, to symmetrical-key encryption techniques. Due to the nature of symmetrical-key type ciphers, it is essential that the technique is reproducible to produce the same results for correct encryption and decryption. To this end, a full sandwich ELISA experiment was measured in order to test for reproducibility first before application to AES. This result can be seen in Figure 4.1. For this, a generic full sandwich ELISA procedure was used for this process, using PBS as the main buffer, PBS-TWEEN as the wash buffer, and 1% BSA as a blocking agent. A diagram of this assay is seen in Scheme 4.1. The dilutions for the secondary antibody are seen in Figure 4.1, the primary antibody and the antigen were both 10 µg/mL. The HRP assay was performed using a citrate buffer pH 5.5, 1 mM ABTS redox dye, and 1 mM hydrogen peroxide. Multiple dilutions of the secondary, conjugated antibody were used to prove that this method would be applicable for different experimental parameters, although the dilution factor is only one of many parameters that may be used. Other parameters that could practically be changed may include, but are not limited to: the amount of the primary antibody, the amount of antigen, pH, and changes in the HRP assay: concentration of substrates, temperature, and wavelength.

4.3.2 Encryption

Since this method was proven to be consistent, it will now be applied for encryption. By taking certain time points, the resulting data values will provide the key. Since AES requires the
input (both key and message) to be in hexadecimal (hex), these values would need to be transformed into hex. In addition, the key length for AES is extremely important. AES runs on keys of set lengths of 128, 192, or 256-bit keys, which equate to 16, 24, or 32 bytes, respectively. Since each hex pair equates to one byte, one will need to choose either 16, 24 or 32 individual points, or to choose a lower number of points and to repeat the key until it is a sufficient length (e.g. use 8 data points for a 8 byte key and repeat it once to have a 16 byte key).

Using the consistent results from the ELISA experiment performed in Figure 4.2, Figure 4.2 shows a single trial of the 2k dilution to be used for encryption. From this, certain predetermined time points are chosen to build the encryption key as seen in Table 4.1. These corresponding points are highlighted in Figure 4.2. To build the encryption key in Table 4.1, data points were chosen from the outside in to illustrate a different sampling technique that can be used. For this technique, the first chosen point is shown first, followed by the last data point chosen, then the second, followed by the second from the end, until all 16 requisite points have been used. The tenths place absorbance values of 16 corresponding time points will be used for the building of the key. This key must then be transformed into hex in order to be used in AES. The given message, consisting of the full title and address of the institution the authors belong to, was also translated into hex for the same reason. Using the AES calculator from Cryptomathic in order to encrypt the message, the
ciphertext is then shown to be “90 34 15 68 27 DB 6E 6C 14 96 88 92 73 AA 01 62 B2 B4 65 2A 48 28 26 07 F4 59 91 C4 1A ED 60 2E A8 C7 78 B8 1D 39 00 5D A8 C2 EC B0 0F 67 41 E8 FF F7 08 F9 42 93 02 1B 5F 9A 53 9C 32 7B C4 5D 1D EC E9 A5 67 56 89 30 78 E4 7B F5 55 1B 12 25 32 68 EE 6F F0 30 A7 AE 5A 9A 8F 3D 32 82 93 E8”. This hex string is the ciphertext that would be sent to the receiver.

4.3.3 Decryption

The receiver then performs the same assay to build their own key seen in Figure 4.3. The receiver then uses the same parameters and time points as the sender in order to make their decryption key in a single trial. Making sure to use the AES calculator in decryption mode, the receiver takes the ciphertext they received and their decryption key to decrypt the original message. As the message is in hex for AES, the message is then transformed back into text and the original message has been correctly decrypted to be the original plaintext message as seen in Table 4.2.

<table>
<thead>
<tr>
<th>Table 4.2: Decryption Process utilizing ELISA data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received message</td>
</tr>
<tr>
<td>77886139D05DABC2ECBD0F67418FF708F9429021B59F9A539C327BC45D31ECE5</td>
</tr>
<tr>
<td>A567569307BE07F555382255268EEF05A7AES9A8F3D32B5318</td>
</tr>
<tr>
<td>Data points 15151524242333</td>
</tr>
<tr>
<td>Data in hex 31 35 31 35 31 35 32 34 34 32 32 32 33 33 33</td>
</tr>
<tr>
<td>Decrypted (hex) 556E6976657273697479206174204616C621616792C20537461746</td>
</tr>
<tr>
<td>5205561697665727369747920666204657730596F72682E2031</td>
</tr>
<tr>
<td>343032057617386696E67746F6E204176652C204616C621616792</td>
</tr>
<tr>
<td>C204E59203132232320A0000000000</td>
</tr>
</tbody>
</table>

4.4 Conclusion

This research demonstrates the use of immunoassay-based experimentation to produce cipher keys for cryptograpic purposes utilizing only one trial of an assay to build a key. As this
process is used to create keys, it may be used with any type of symmetrical-key encryption method as long as the manual of parameters for each person describes the correct key length. By utilizing this methodology in order to properly encrypt and decrypt a message using the current encryption standard AES, this research shows a proof-of-concept allowing for immunoassays to be used to higher levels of encryption than they have been used in prior. By not repeating parameters to make each subsequent key, the robustness of the security in this method is enhanced as it is more difficult to break the cipher if the key is not repeatedly used in any other messages. The versatility of this method by having a large sum of parameters that may be changed as it technically consists of an antibody-antigen-antibody interaction in addition to an enzymatic assay, allows for a multitude of potential unique keys to be able to be produced. The methodology presented here provides an alternative way the production of cryptographic keys rather than the use of a random number generator.
5. Biometrics for Asymmetric Cipher

Adapted in part with permission from McGoldrick, L. K., Hair, M. E., Halámek, J. “Biometrically Derived Keys for Asymmetric Encryption: Data Encryption and User Authentication”. Manuscript in Preparation

5.1 Introduction

This proof-of-concept work shows that biometric data made from the metabolite levels in one’s sweat can be used in an asymmetrical-key cryptographic system. To this end, by using an individual’s levels of lactate and urea in sweat, one can create two keys that are to be used for an asymmetrical-key cipher. Demonstrated here are both uses for this type of cipher, data encryption and user authentication, which are both essential in data security. An asymmetric cipher, kRSA, was used to use this biometric data in order to encrypt and decrypt a small message and also to produce an electronic signature.

Currently, symmetrical-key ciphers are the primary method of encrypting and decrypting large amounts of data and messages\(^1-3\). Our research group has focused on multiple types of chemical techniques in order to encrypt data using a symmetrical-key cipher system\(^75\). Depending on the type of cipher system used, more specifically the encryption method, the level of security changes due to the complexity of some algorithms currently in use. However, as these symmetrical-key ciphers have many advantages in speed, security, robustness, and ease of use, they have one main drawback-the key. This is due to the requirement of symmetrical-key ciphers to have each person, the sender and the receiver(s) of a message, use the same exact key for a particular message. The problem is the secure transmission of this key between parties, as using another symmetrical-key cipher to send the key would pose the same problem. This is alleviated by the use of asymmetrical ciphers. In current communication, a hybrid technique is actually used, where a symmetrical-key cipher is used to encrypt the bulk message and an asymmetrical-key
cipher is used to transmit the key for the symmetrical-key cipher\textsuperscript{1–3,91}. This is due to asymmetrical-key ciphers being significantly slower than their symmetrical-key counterparts.

Biometrics, the measurements of bodily identifiers and physical characteristics, have been studied for the use of both encryption\textsuperscript{55,92–95} and other security concerns, namely authentication\textsuperscript{96–98}. Biometrics are also commonly referenced in pop culture using retinal scans, fingerprints, gait, and other characteristics for “advanced” security systems. The use of biometrics causes apprehension in cryptographers for use in cryptography, especially as keys, as some biological measurements in a person change from day to day and may depend on certain other characteristics. This issue is referred to as fuzzy\textsuperscript{99–101} biometrics and is used in some methods for encryption. The problem however is with the “fuzzy biometric logic versus absolute mathematical logic problem”\textsuperscript{1}. The other problem with biometrics as keys is if the biometric is stolen, it is very difficult to replace. It is very difficult to replace one’s eye or finger if that is the key; not that those would be cut off as seen in film, but much more likely that the corresponding electronic data is mimicked. The approaches mentioned above mainly look at the use of biometrics as direct keys for cryptography. The method presented here alleviates these issues. In this research this issue is reduced, if not eliminated, as the biometric details are used to derive the key but are not used as the key itself. This distinction adds a layer of security to the use of the biometric data and also allows for the method of key development to be changed if the key is ever compromised, as it is difficult to back-calculate the initial integers in asymmetric key derivation protocols.

5.2 Materials and Methods

5.2.1 Chemicals
The following enzymes were purchased from Sigma-Aldrich: lactate oxidase (LOx, E.C. 1.13.12.4), horseradish peroxidase (HRP E.C. 1.11.1.7), urease from jack bean type III (UR, E.C. 3.5.1.5), and L-glutamic dehydrogenase from bovine liver type II (GIDH, E.C. 1.4.1.3). The following chemicals were also purchased from Sigma-Aldrich: L-Lactate, 2,2′-azino-bis(3-ethylbenzothiazoline-6-sulfonic acid) [ABTS], potassium phosphate dibasic, potassium phosphate monobasic, urea, β-nicotinamide adenine dinucleotide reduced dipotassium salt (NADH), α-ketoglutaric acid disodium salt dehydrate (KTG), and Trizma® base. Hydrochloric acid was purchased from EMD Millipore. All experiments use ultrapure water (18.2 MΩ·cm) from an ELGA PURELAB Flex water purification system. Analysis of the enzymatic assays were performed on a Molecular Devices SpectraMax Plus 384 UV/Vis spectrophotometer. Sweat collection was performed as a variation of the Gibson and Cooke method\textsuperscript{102} based on the iontophoresis of pilocarpine to induce sweating. Additional details can be seen in Hair\textsuperscript{103}. This involved pilocarpine nitrate salt from Sigma-Aldrich, an Eventek DC power supply, a Leeds & Northrup Co. AC-DC decade resistor, and EKG limb clamp electrodes for sweat generation. Sweat collection was performed using Coach sports tape, 5.1 cm x 5.1 cm Equate gauze pads, and polyethylene film.

5.2.2 Enzymatic Assays

Sweat samples were obtained from two individuals to build two sets of asymmetric key pairs. These sweat samples were produced utilizing a modified version of the Gibson and Cooke method\textsuperscript{102} described in Hair\textsuperscript{103}. Enzymatic assays for lactate, using lactate oxidase (LOx) and horseradish peroxidase (HRP), are shown in Scheme 5.1.
oxidase and horseradish peroxidase, and urea, utilizing L-glutamic dehydrogenase and urease, were performed to provide the biometric data\textsuperscript{97}. The assay performed for lactate can be seen in Scheme 5.1 and the assay for urea can be seen in Scheme 5.2.

The assay for the detection of lactate first uses the enzyme lactate oxidase (LOx) in order to convert lactate and oxygen into pyruvate and hydrogen peroxide. Horseradish peroxidase (HRP) then reduces the peroxide into water while oxidizing a redox dye indicator, the methodology outlined here using ABTS as the redox dye. ABTS in its oxidized state is recorded spectrophotometrically at 405 nm.

Similarly for the detection of urea, urease uses the substrates of urea and water to produce carbon dioxide and ammonium. These ammonium ions, along with ketoglutarate and NADH are used as substrates for the second enzyme, glutamic dehydrogenase (GIDH) in order to produce glutamate, water, and NAD\textsuperscript{+}. The change of NADH to NAD\textsuperscript{+} can be measured as a decrease in absorbance at a wavelength of 340 nm.
5.2.3 Cipher

The main use of asymmetrical-key ciphers is message encryption. To this end, “Bob” releases his public key onto the internet. “Alice” sees the key and wants to send Bob a secure message. Alice takes Bob’s public key, encrypts a message with it and sends that message to Bob. Bob then uses his private key to decrypt the message. This is seen in Scheme 5.3.

By performing a similar process, one can also address the issue relating to authentication by making a digital signature. In a very basic version of this technique, the sender, Alice, would take a section of her message to Bob, encrypt it with her own private key, and send this to Bob. As Bob knows her public key, as it is public information, he can authenticate that it truly was Alice who sent the message in question by using this digital signature method. This process is illustrated in Scheme 5.4.

The method presented in this paper focuses on the application of biometric data in order to produce the keys for an individual as seen in Scheme 5.5. Using the biometric data from a person’s sweat for two particular metabolites, individualized keys will be created for each person and used for both message encryption and authentication as discussed in the previous paragraph. This methodology will use two different metabolites, lactate and urea, which have been analyzed by other members of this research lab\textsuperscript{97}. As this is a proof-of-concept, a simpler version of the RSA asymmetric cipher will be used\textsuperscript{66}, Kid RSA or kRSA\textsuperscript{91,104}. Neil Koblitz created this cipher in order to introduce cryptography to secondary school students\textsuperscript{104}. kRSA
consists of choosing four integers, which are then used to create the public and private keys. By using these keys, along with base 26 versions of a message text, one can send a message. In addition, by following the other procedure above, this method can be used for authentication.

5.3 Results and Discussion

5.3.1 Reproducibility and variation check

Lengthy laboratory and statistical analysis was performed in prior research into the biometric analysis of sweat using the methodology utilized here.97

5.3.2 Encryption

These assays were run for each individual over a two-day period, providing four integer numbers for each person. These four numbers, two relating to the level of lactate and two relating to the level of urea in each of the individuals, would be used to produce that individual’s pair of keys for asymmetric encryption. For Koblitz’s kRSA, one uses those four integers (a, a’, b, b’) to produce four values: M, which is used in calculations for the other three; e, the public key, also referred to as the encryption key; d, the private key, or the decryption key; and lastly n, which is also used in both encryption and decryption. The equations for these can be seen in Equations 5.1-5.4.

Firstly, in order to show an example of asymmetrical-key encryption of a message, this process will be demonstrated using individual 1’s results. The biometric results from the assay of lactate (in mM) will provide a and b, and urea (the mM result multiplied by 10 to give a matching
From these four integers, the kRSA values were produced as seen in Table 5.2 using the calculations in Equations 5.1-5.4. As stated previously, e is individual 1’s public key and d is their private key. Individual 1 releases this public key, e, and their value for n in order for individual 2 to send them a message.

For individual 2 to send an asymmetrically encrypted message to individual 1, the process outlined in Scheme 5.3 will be used—with individual 1 being “Bob” and individual 2 being “Alice”. For kRSA, the type of asymmetric encryption to be used for this example, the sample message must first be changed into Base 26. This was done using dcode’s “Base 26 Cipher”\(^{105}\) in the mode recommended for cryptography. A short sample message, “HELP” was changed using this process and became “144316”. This is the message that Alice (individual 2) wants to send to Bob (individual 1). This message is then encrypted using Equation 5.5, with ct being the ciphertext or the encrypted text, m being the message in Base 26, and e and n from Table 5.2. The ciphertext would then be “7025890” using Bob’s public key, e, and n. Directly translated using Base 26, this ciphertext would read “OISHN”, showing that it did encrypt the message. Alice would then send this message to Bob, who would be the only one with the knowledge of his private key to decrypt it.

### 5.3.3 Decryption
To decrypt this message, Bob uses his private key, \( d \) and his value for \( n \) according to Equation 5.6. By using Equation 5.6, the plaintext original message, \( m \), is subsequently produced. For the example here, \( m \) is calculated to be “144316”, which correctly corresponds to “HELP”.

\[
ct = m \cdot e \mod n \\
\text{Encrypted text} \\
m = d \cdot ct \mod n \\
\text{Decrypted text}
\]

Scheme 5.6: Simplified outline of kRSA message encryption

With this example of the process outlined above, it was demonstrated that a short message was successfully encrypted, sent, and decrypted utilizing kRSA with keys which were derived from Bob’s (individual 1’s) biometrics. This process is outlined in Scheme 5.6.

5.3.4 Signature for Authentication

As authentication is also important, this same asymmetric-key cipher with biometrically derived keys will be used in order to show an example of how Alice can use her asymmetric keys in order to authenticate her identity in sending this message to Bob.

As stated previously, the other use for asymmetric encryption is user authentication via the use of signatures. In this process, Alice (Individual 2) aims to make sure that Bob knows that it is truly her sending him the above message. This process, outlined in Scheme 5.4 above, will require Alice’s set of asymmetric keys derived from her biometric data. Using the same assays as Bob, a set of the same four biometrics were measured as seen in Table 5.3. Table 5.4 shows Alice’s four values for use in kRSA calculated using Equations 5.1-5.4, similarly to Bob’s values. As illustrated
in Scheme 5.4, for a signature following this process will switch the order of the keys being used. For the encryption of the signature, Alice will use her private key, d, and for decryption of that signature Bob will use her public key, e.

For her signature, “ALICE”, Alice first transforms it into Base 26, giving her a value of “674055”. Using the encryption calculation shown in Equation 5.7, which is analogous to Equation 5.5. By performing this, Alice has now encrypted her signature to be “6507723”. In Base 26 this is “NFFUA”. In this example, Alice would then send this along with her message above to Bob.

Bob then uses Equation 5.8, which is analogous to Equation 5.6, to decrypt the signature with Alice’s public key. By performing this decryption Bob calculates “674055”, or “ALICE”, showing that it truly was Alice who sent him this message. Scheme 5.7 shows a short outline of this process. The above steps show that one is also able to use this process to not just send messages, but also to be used for user authentication via a digital signature, which are the two main purposes of asymmetric encryption.

5.4 Conclusion

This proof-of-concept research shows that by utilizing biometric data from a person, one can use asymmetrical-key cryptography techniques to generate keys derived from biometric data in order to be used for both processes of asymmetric ciphers: message encryption and user authentication. Shown in this manuscript are examples of both uses of asymmetric encryption, which demonstrates that this methodology is fully viable for use in basic asymmetric encryption. Ideally, the integers used for a higher level asymmetric cipher, for example RSA instead of kRSA,
would be hundreds of digits long for them to be completely secure in those cipher systems\textsuperscript{1,3,104}. For this to be achievable, more biometrics could be taken and strung together in order to make up those extended integers to be used in key generation. By using biometric data, these sets of values would be unique for each person, enabling a secure methodology of key generation. As these numbers are strung together detailing different biometrics of a person, if a key ever is compromised it may be easily replaced with a new key by rearranging the order of each biometric in the string.
6. Conclusions

Each research project within this dissertation aimed to use different biochemical and chemical methodologies to offer different alternatives to a random number generator for cryptological purposes. The projects use different cryptographic ciphers for encryption to show viability and resilience of the methodologies within and how they relate to current cryptographic technologies. From using basic addition and subtraction to the current standard of encryption, AES, the research presented here was able to perform encryption of messages that were able to be properly encrypted. In addition, a symmetrical-key and asymmetrical-key ciphers were used to show both types of ciphers used currently.

The first project involved the use of three enzymatic assays to create the keys for a basic addition/subtraction symmetrical-key cipher. When both the sender and receiver of a message perform the same designated experiment under identical conditions, proper encryption and decryption occur. It is important that both parties perform the same exact experiment as this is a symmetrical-key cipher system. This work demonstrates bioaffinity-based assays are a viable method to use for the formation of cryptographic keys in a symmetrical-key cipher process. As it is important to use new keys for each individual message, the variability of the enzymatic assays involved with this research, in addition to the multitude of other enzymatic assays available, allow for one to produce a new key each time. For example, using a different set of assays, or changing the parameters of the experiment, or changing the time points chosen are all viable method for producing a new key. The other projects within are a continuance of this work for other biochemical and chemical methodologies.
Secondly, a common electrochemical experiment was adapted for use with the current standard cipher for encryption, AES. A cyclic voltammetry experiment involving the oxidation and reduction of ferrocyanide/ferricyanide was measured and used for the symmetrical-key cipher, AES. As with the first project, it was demonstrated that if two people perform the same experiment under the same conditions, accurate encryption and decryption will occur. A sample message was encrypted and decrypted utilizing this method. This research not only proves that a CV experiment is also viable for encryption in general, but also that it is viable for the current standard for encryption, AES, which is very stringent with the requirements for the key compared to the previously used addition/subtraction. The Halámek Lab will continue this work by combining electrochemistry with a bioaffinity-based assay to further broaden the potential methodologies for the derivation of cipher keys.

Bioaffinity-based assays were then tested using a different assay technique involving an immunoassay to encrypt a message with AES once again, as AES is the current standard for encryption. By using the results from a full-sandwich ELISA type of immunoassay, a message was accurately encrypted and decrypted through AES. This project provides yet another viable method for the origination of cipher keys. Similarly to the enzymatic techniques mentioned previously, there are many variants of this method that can be used to produce a new key every time. By using different parameters in any step of the process, including the enzymatic assay to produce the actual colorimetric result, would result in a new key. The Halámek Lab will further this research by utilizing different immunoassay techniques other than ELISA for the purposes of encryption.

For the final research project an asymmetrical-key cipher was used for encryption. This allows not only for the encryption of short messages but also for user authentication. This project was an expansion of prior research performed in the Halámek Lab as it combined the previous use
of sweat biomarkers for biometric purposes\textsuperscript{97} and applied those methods for encryption. Through these methods involving the use of enzymatic assays to determine the amount of certain metabolites in sweat, keys for use in an asymmetrical-key cipher can be produced for individuals through the use of techniques relevant to the asymmetrical-key cipher being used. In this case, a rudimentary form of the RSA cipher was used, kRSA, as it is easier to understand since it was made for the introduction of cryptography for high school students. Accurate encryption and decryption were performed for both a short message and the separate encryption of a “signature” for user authentication using sweat biomarker analysis to produce both public and private keys for two individuals. This research targeted both main issues with data transfers in the digital age: message security and user authentication. This research further showed that not only can a person’s sweat be used in cryptography to determine the values of a cryptographic key, but to be used for an asymmetrical-key cipher as well as the previously researched symmetrical-key cipher systems. Conversely to previously mentioned, a new key is not required each time for an asymmetrical-key cipher system as long as the key is not stolen and is stable enough to not be back-calculated or guessed from the public version. However, if a new key was necessary, different parameters. The Halámek Lab will further this research by examining biometric techniques in combination with other logic and asymmetric cipher systems.
Appendix

Publications by the author


Presentations by the author

Oral Presentations


Poster Presentations


References


(20) Karlsson, R.; Michaelsson, A.; Mattsson, L. Kinetic Analysis of Monoclonal Antibody-


ELAN1110>3.0.CO;2-E.


Reuse Permissions