Security Suite: EECS 444 Final Project

KIM ALMCRANTZ, Destroyer of Worlds
MARK LALOR, Eater of Nightmares
BRIAN LI, Summoner of Flames
VANESSA MELIKIAN, Reaper of Souls
MAYA NAYAK, Tormentor of the Lost
JACOB WISE, Annihilator of the Innocent

This is our abstract. Currently it is empty because no one has written it. In order to make it not empty, it must be written/

Additional Key Words and Phrases: encryption, cipher, hash, entropy

ACM Reference Format:
Kim Almcrantz, Mark Lalor, Brian Li, Vanessa Melikian, Maya Nayak, and Jacob Wise. 2018. Security Suite: EECS 444 Final Project. 1, 1 (December 2018), 4 pages. https://doi.org/0000001.0000001

1 INTRODUCTION

To begin, we ponder a quote from an anonymous philosopher.

> "where's brian ".

What does it mean? Who said it? Why was it said? We may never know. But what we do know is the following:

This article is divided into several sections, in Section [1], we introduce the cryptographic environment that we will explore. In Section [2] we describe implementations of several symmetric and asymmetric encryption algorithms, and then Section [3] we present our tool SecuritySuiteGUI, a software suite to experiment with these implementations. We then demonstrate the power of password cracking with a hashcat demo in Section [4]. Finally, we demonstrate how the Vigenère cipher may be easily cracked with computational power in Section [5]. We evaluate our methods in Section [6], and then discuss our techniques, challenges, and other thoughts in Section [7]. Finally, we discuss our final conclusions in Section [8].

- To the best of our knowledge, this is not the first time something like this was developed
- We use [1], for a chocolate chip cookie recipe.

1.1 Basic Crypto Stuff

This is a talk about all the types of ciphers, symmetric, asymmetric, maybe more!

Here is the structure of the a bad algorithm:

(1) Break into blocks of size $k = \frac{n^7}{8}$

Authors' addresses: Kim Almcrantz, Destroyer of Worlds, kaa97@case.edu; Mark Lalor, Eater of Nightmares, mwl58@case.edu; Brian Li, Summoner of Flames, bvl8@case.edu; Vanessa Melikian, Reaper of Souls, vlm21@case.edu; Maya Nayak, Tormentor of the Lost, mkn30@case.edu; Jacob Wise, Annihilator of the Innocent, jsw107@case.edu.

XXXX-XXXX/2018/12-ART $15.00
https://doi.org/0000001.0000001

ALGORITHM 1: FakeDES implementation

Input: Binary plaintext message m, a binary encryption key k
Output: Binary ciphertext message c
$c = m \times k$ **repeat**
    $c = mc^2$
until $\pi > -1$;

(2) Encipher each block with magic
(3) Do XOR magic
(4) Implement DES

2 CRYPTOGRAPHIC ALGORITHM IMPLEMENTATIONS

2.1 FakeDES

As Algorithm 1 states, DES is a symmetric encryption algorithm with steps.

2.2 RSA

RSA is asymmetric!

2.3 md5

Md5 is a hash algorithm!

3 SECURITYSUITEGUI

3.1 Goals

Some description:

Lemma 3.1 (Lemma Subhead). *The solution to the C-MWPC problem is no worse than the solution to the MWPC.*

Proof. Simply, any solution to the MWPC is also a solution to the C-MWPC. But some solutions to C-MWPC may not apply to the MWPC (if any coalescing were made). □

4 HASHCAT DEMO

Words go here!

5 VIGENÈRE CIPHER CRACKER

Words go here too!

6 EVALUATION

Evaluation, efficiency? Challenges?

7 DISCUSSION

What didn't we cover? :O

8 CONCLUSIONS

We conclude that cryptography is very useful! $\frac{10}{10}$ would reccommend.

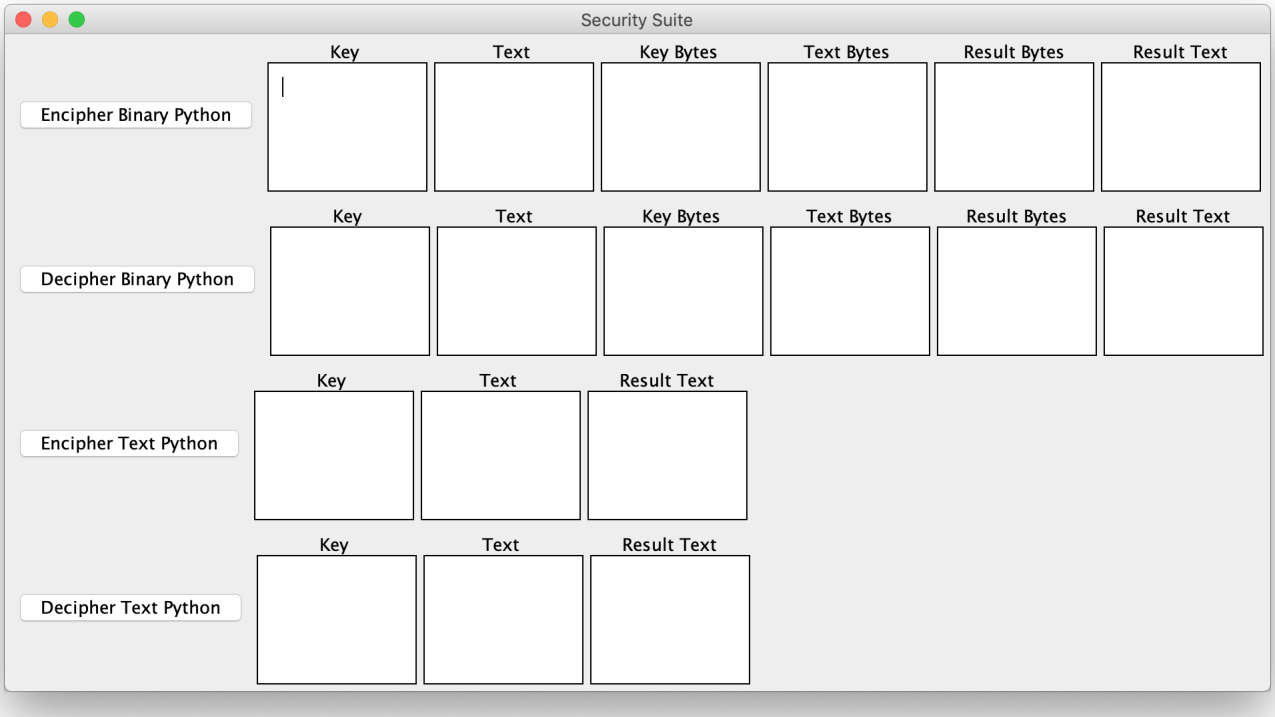

Image of our demo tool

Fig. 1. Image of the security suite demo tool.

9 REFERENCES SAMPLES

A couple of citations with DOIs: [2, 3]. Online citations: [4–6].

A ELABORATION ON THE ABCD ALGORITHM

This is an appendix, maybe about some equation

$$P = NP$$

B SUPPLEMENTARY MATERIALS

B.1 Hashcat materials

Materials?

B.2 Tool: Symmetric Ciphers Online

Link

ACKNOWLEDGMENTS

The authors would like to thank the mitochondria for being the powerhouse of the cell.

REFERENCES

[1] A. Adya, P. Bahl, J. Padhye, A.Wolman, and L. Zhou. 2004. A multi-radio unification protocol for IEEE 802.11 wireless networks. In *Proceedings of the IEEE 1st International Conference on Broadnets Networks (BroadNets'04)*. IEEE, Los Alamitos, CA, 210–217.

[2] IEEE 2004. IEEE TCSC Executive Committee. In *Proceedings of the IEEE International Conference on Web Services (ICWS '04)*. IEEE Computer Society, Washington, DC, USA, 21–22. https://doi.org/10.1109/ICWS.2004.64

[3] Markus Kirschmer and John Voight. 2010. Algorithmic Enumeration of Ideal Classes for Quaternion Orders. *SIAM J. Comput.* 39, 5 (Jan. 2010), 1714–1747. https://doi.org/10.1137/080734467

[4] Harry Thornburg. 2001. Introduction to Bayesian Statistics. Retrieved March 2, 2005 from http://ccrma.stanford.edu/~jos/bayes/bayes.html

[5] TUG 2017. Institutional members of the TEX Users Group. Retrieved May 27, 2017 from http://wwtug.org/instmem.html

[6] Boris Veytsman. [n. d.]. acmart—Class for typesetting publications of ACM. Retrieved May 27, 2017 from http://www.ctan.org/pkg/acmart