Roman Nicolai
December 8, 2019
ICS 222

Full Report

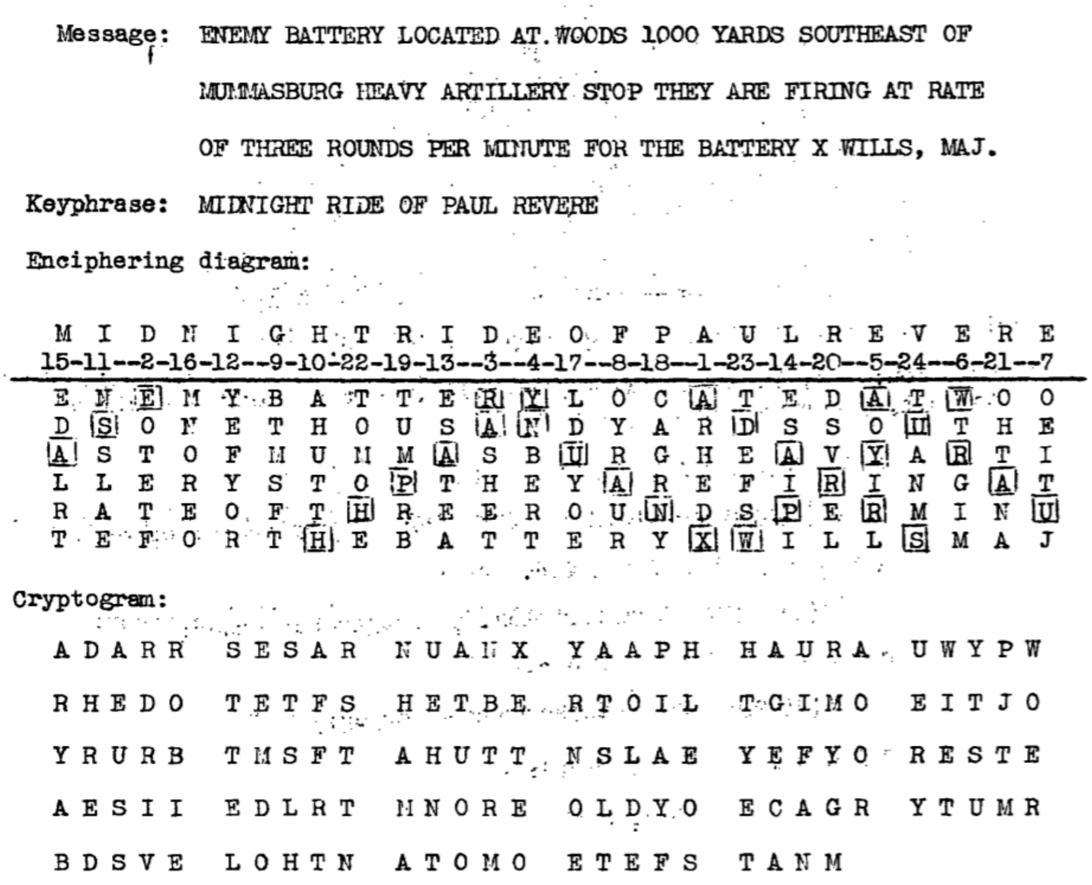
Over the length of ICS 222 I have expanded upon my knowledge of cryptography. I gained more of an understanding of the mathematical foundations that underlie cryptography. I also gained some information in regards to the history and development of cryptography, as well of its prominence today. Effectively, cryptography can be defined as the encompassing techniques for secure communication in the presence of third parties.

I will begin with the history of cryptography as that should provide a background to the rest of this report. The beginnings of "cryptography" as a term dates back to only as recently as the 19th century where "cryptograph" was used in a novel by Edgar Allan Poe. However, prior to the modern age, cryptography was essentially synonymous with encryption. Encryption refers to the process of converting ordinary, readable information into an unintelligible form known as ciphertext. A cipher is a pair of algorithms that are used to encrypt the information and vice-versa decrypt the same information. These cipher algorithms are today interchangeable with the common term "key".

Therefore, older cryptographic methods were effectively only encryption methods. Cryptographers, such as those in the military, would be tasked with encrypting and decrypting messages. Going back further, classical cyphers were primarily limited to transposition cyphers and substitution cyphers, which are both very similar to one another. Transposition cyphers rearrange letters in a message, while substitution cyphers rearrange groups of letters with other groups of letters. Today, we don't typically see these classical cyphers in use, other than fun hobby puzzle use by enthusiasts.

By the time World War I came around, many new mechanical encryption devices were invented. These new ciphers implemented a higher quality in cryptanalytic soundness, however they were still only limited to encryption and decryption. These newer techniques were used throughout World War I and World War II.

Here is an example of older military cryptography, given in ADVANCED MILITARY CRYPTOGRAPHY; 1931 EDITION, SPECIAL TEXT NO. 166 (page 8) :



Message: ENEMY BATTERY LOCATED AT.WOODS 1000 YARDS SOUTHEAST OF MUMMASBURG HEAVY ARTILLERY STOP THEY ARE FIRING AT RATE OF THREE ROUNDS PER MINUTE FOR THE BATTERY X WILLS, MAJ.

Keyphrase: MIDNIGHT RIDE OF PAUL REVERE

Enciphering diagram:

```
 M  I  D  N  I  G  H  T  R  I  D  E  O  F  P  A  U  L  R  E  V  E  R  E
15-11--2-16-12--9-10-22-19-13--3--4-17--8-18--1-23-14-20--5-24--6-21--7
-----------------------------------------------------------------------
 E  N  E  M  Y  B  A  T  T  E  R  Y  L  O  C  A  T  E  D  A  T  W  O  O
 D  S  O  N  E  T  H  O  U  S  A  N  D  Y  A  R  D  S  S  O  U  T  H  E
 A  S  T  O  F  M  U  M  M  A  S  B  U  R  G  H  E  A  V  Y  A  R  T  I
 L  L  E  R  Y  S  T  O  P  T  H  E  Y  A  R  E  F  I  R  I  N  G  A  T
 R  A  T  E  O  F  T  H  R  E  E  R  O  U  N  D  S  P  E  R  M  I  N  U
 T  E  F  O  R  T  H  E  B  A  T  T  E  R  Y  X  W  I  L  L  S  M  A  J
```

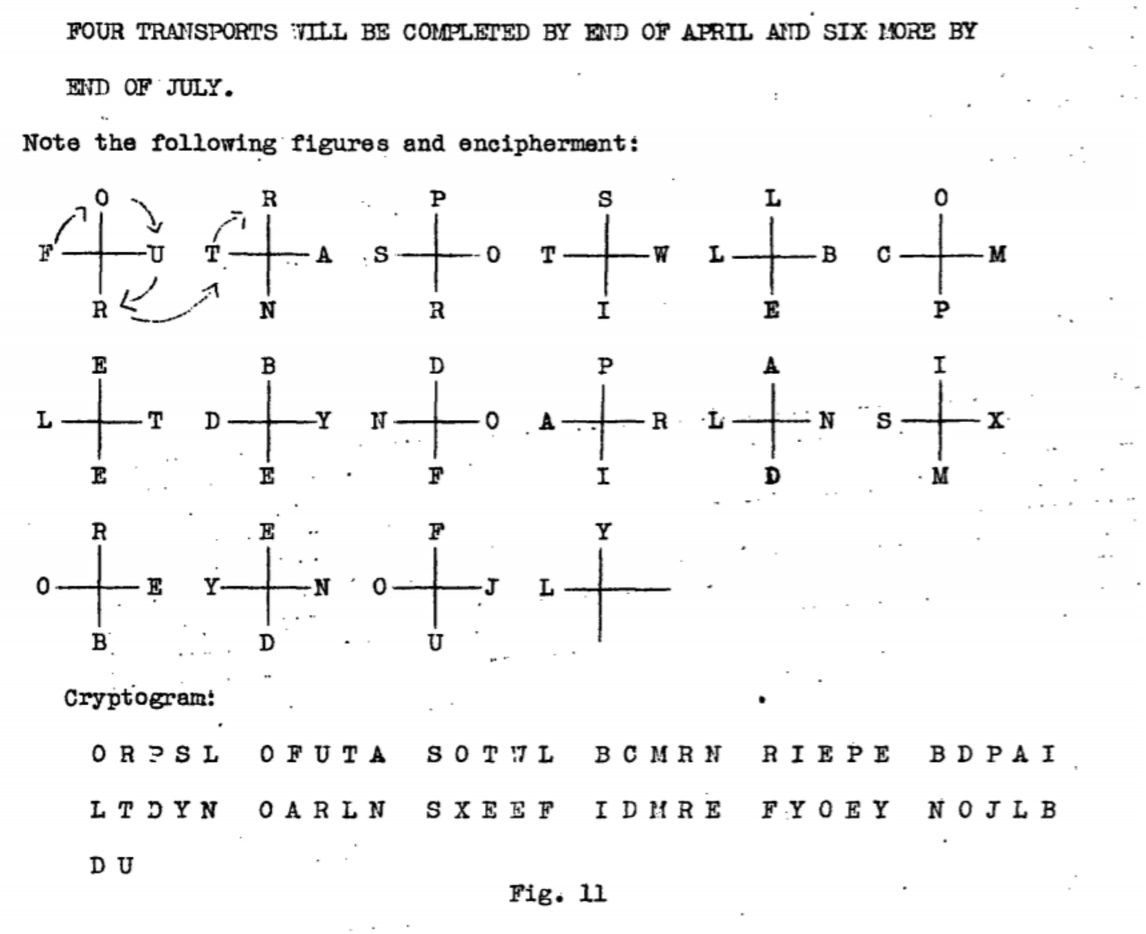
Cryptogram:

```
ADARR  SESAR  NUANX  YAAPH  HAURA  UWYPW
RHEDO  TETFS  HETBE  RTOIL  TGIMO  EITJO
YRURB  TMSFT  AHUTT  NSLAE  YEFYO  RESTE
AESII  EDLRT  MNORE  OLDYO  ECAGR  YTUMR
BDSVE  LOHTN  ATOMO  ETEFS  TANM
```

Fig. 6

This uses what is called a diagonal method. It is a method involving diagonal transpositions which is reported to have been employed by the French Army in the World War. I do not want to go to in-depth on the explanation on this because the text gives the same explanation. Check it out if you would like to learn more.

Here is another example from the same text (page 14) :



FOUR TRANSPORTS WILL BE COMPLETED BY END OF APRIL AND SIX MORE BY END OF JULY.

Note the following figures and encipherment:

Cryptogram:

O R P S L O F U T A S O T W L B C M R N R I E P E B D P A I

L T D Y N O A R L N S X E E F I D M R E F Y O E Y N O J L B

D U

Fig. 11

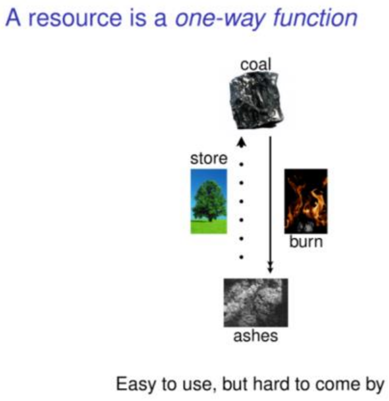
I thought this was an interesting application therefore I chose it as an example. It falls into the category of "Transposition methods using special figures". This caught my attention because of the different visual, but also the use-case. This method is only useful in special cases where the correspondence is restricted to very brief communications to a limited number of persons. In order for this method to be effective, those involved must be acquainted in advance with the certain criteria. I found this method to be easier to understand in comparison to the others, which may be why it was only used very situationally.

Feel free to read through the rest of the source. There are many examples of older military cryptography techniques. I found many of them quite difficult to figure out, even with the description, which goes to show that they likely were quite effective in obscuring communications. A lot of time and critical thought seem to have been put into these schemes.

As we moved deeper into the 20th century and closer to modern times, cryptography as an application evolved. The most prominent change was the shift from mere encryption to a wider, more extensive application of mathematics. Going back to my previous military examples, though these were well thought-out, they still only made use of encryption and decryption. Essentially, these were only linguistic and lexigraphical manipulations. With help from an advance in technology, modern cryptography now encompasses information theory, computational complexity, statistics, combinatorics, abstract algebra, number theory, and finite mathematics. Extensive open academic research into cryptography is relatively recent; it began only in the mid-1970s. Research into integer factorization, discrete logarithm problems, and cryptographic hash functions has lead to breakthroughs in cryptography. Today we have the use of these underlying mathematics in our daily lives, through our computer networks and computer security systems, among other things.

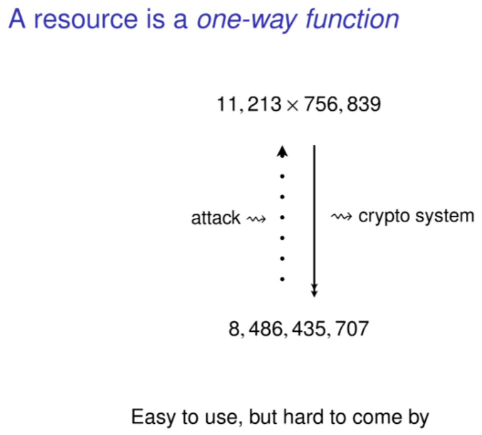
In ICS 222, we approached concepts relating to modern cryptography only later in the course. The fifth and final concept we were exposed to was Resource. Resource makes use of all previous concepts (induction, coinduction, computability, metaprogramming) to ultimately lead up to complexity.

In the course slides, we are given examples of functions that could have cryptographic applications. One-way functions are useful in cryptography because, as one can assume, they are a function that is easy to send information "one-way" but is hard to reverse and read in the opposite. The examples in the slides start off with one-way functions that are easy to understand, but gradually become more numerical.


A resource is a *one-way function*

Easy to use, but hard to come by

Non-renewable natural resources are a good example of a one-way function



A resource is a *one-way function*

11, 213 × 756, 839

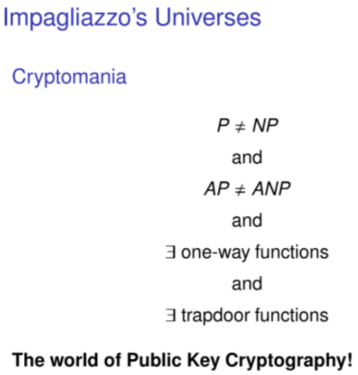
attack ⇝

⇝ crypto system

8, 486, 435, 707

Easy to use, but hard to come by

Multiplication of primes is "easy", factoring is "hard". It forces an exhaustive search.



Impagliazzo's Universes

Cryptomania

$P \neq NP$

and

$AP \neq ANP$

and

∃ one-way functions

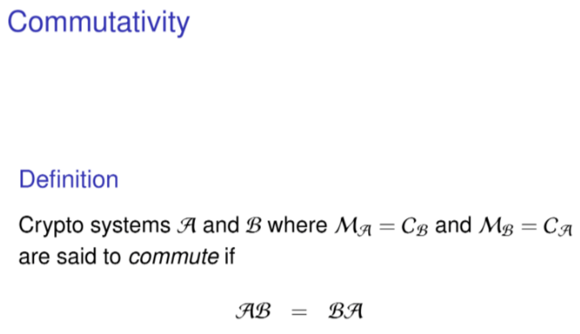
and

∃ trapdoor functions

The world of Public Key Cryptography!

Trapdoor is the key to a one-way polynomial function.

Related to the class, cryptography only became "computable" recently because of new complexities derived from mathematics and hardware. I would like to mention William Frederick Friedman. Friedman was a US Army cryptographer who ran the research division of the Army's Signal Intelligence Service in the 1930s, and parts of its follow-on services into the 1950s. He was a very compelling and pivotal figure in the history of cryptography. However, as I mentioned earlier, there was no computability in cryptographic practice before 1980s. None of Friedman's crypto systems survive .03 sec of linear cryptanalysis on a laptop today. The problem is that they are commutative (related to the issue of encryption/decryption limitation). New technology moved away from commutativity to what we have presently.



Commutativity

Definition

Crypto systems $\mathcal{A}$ and $\mathcal{B}$ where $\mathcal{M}_{\mathcal{A}} = C_{\mathcal{B}}$ and $\mathcal{M}_{\mathcal{B}} = C_{\mathcal{A}}$ are said to *commute* if

$$\mathcal{A}\mathcal{B} = \mathcal{B}\mathcal{A}$$

Beyond this class I would like to use the techniques we have learned to analyze cryptosystems more in-depth. We have learned various counters to help get a sense of complexity. For example, we have learned time, space, and bound complexities which are all decidable complexities. These counter complexities can be used in measuring a system. Also I want to note Professor Pavlovic provided some information on current trends in cryptography today. Cryptography is not studied as much today in security because there are much easier things to attack. The NSA used to have many more people studying cryptography, but today has much less of a focus. Concluding, the evolution of cryptography was certainly a fascinating one. It's complexity today compared to even fifty years ago is astounding. Where it will be in the next decade or two will certainly be something I would like to keep track of.

See next page for Works Cited

Works Cited

1. *Advanced Military Cryptography. 1931 Edition* . NSA, www.nsa.gov/Portals/70/documents/news-features/declassified-documents/friedman-documents/publications/FOLDER_239/41748809078800.pdf.
2. Kahn, David. *The Codebreakers: the Comprehensive History of Secret Communication from Ancient Times to the Internet*. Scribner's and Sons, 1997.
3. Pavlovic, Dusko. " ICS 222: 5. Complexity Dusko Pavlovic Self-Program Measures Cryptomania Outsmarting Lesson Basic Concepts of Computation: Fifth Concept: Complexity (Concerning Computational Resources)." *Http://Www.asecolab.org/Courses/Ics-222/,* Aug. 2019, www.dropbox.com/s/p3upixjmmeeuk1z/5000-main.pdf?dl=0.
4. Pavlovic, Dusko. "ICS 222 Lecture." Nov. 2019, Honolulu, Sakamaki Hall.