Cryptography is Cool

By: Huy Pham, Khanh Lam, Oanh Duong and Carol Manlangit

INTRODUCTION

What is cryptography?

Cryptography is the art of transforming data into unreadable format (encrypting) and translating it back to real format (decrypting) by only the people who have access to the key.

When is cryptography used?

Cryptography has been used by many throughout the history of mankind: from Egypt's Old Kingdom to Greeks of Classical times, from World War I to the present time to serve the purpose of "codes breaking" and "cipher."

Why is it important?

Cryptography is used for many reasons including: information technology and security purposes. It is an advancement of our technology and helps secure confidential information.

METHODS

Here's the scenario:

3 days before the poster project is due, we have still not come to terms with the details. We have a message to send to our professor, but how are we going to pull it off?

We know we need a matrix code that each of the four of us knows by heart. It must also be invertible. So our code matrix is square, with linearly independent columns such that its determinant is any value other than 0.

METHODS CONTINUED..

The question is how are we going to have numbers fill our code matrix?

The 26 letters of the English alphabet must be assigned to the numbers 0 to 26, with number 0 being the space.

Space = 0

A=1, B=2, …, Z=26

METHODS CONTINUED..

We thought hard about what kind of message to encrypt. After finally choosing a matrix M for our message, we encrypted it by multiplying $A \times M$ to get an encrypted matrix B.

In order to decrypt matrix B and reveal the message, you must have access to matrix A.

RESULTS

We decided to insert the initials of our first names into the diagonal of our code matrix:

$$A = \begin{bmatrix} 11 & 1 & 2 & 3 \\ 0 & 8 & 4 & 5 \\ 0 & 0 & 15 & 6 \\ 0 & 0 & 0 & 3 \end{bmatrix}$$

B is the encrypted matrix that we are sending out electronically:

$$B = \begin{bmatrix} 127 & 47 & 114 \\ 217 & 148 & 240 \\ 69 & 285 & 297 \\ 27 & 0 & 36 \end{bmatrix} \equiv \left(\begin{bmatrix} 19 & 20 & 6 \\ 1 & 13 & 24 \\ 15 & 15 & 0 \\ 0 & 0 & 9 \end{bmatrix} \right) \bmod 27$$

[A] serves the purpose because the matrix of this family is invertible.

We challenge everyone to decode our message.

RESULTS CONTINUED…

In order to decode the encrypted matrix B, we use the inverse of A to transform B to a decrypted matrix (the original message).

To find A^{-1}, we row reduce:

$$\begin{bmatrix} 11 & 1 & 2 & 3 & 1 & 0 & 0 & 0 \\ 0 & 8 & 4 & 5 & 0 & 1 & 0 & 0 \\ 0 & 0 & 15 & 6 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & 0 & \frac{1}{11} & \frac{-1}{88} & \frac{-1}{110} & \frac{-71}{1320} \\ 0 & 1 & 0 & 0 & 0 & \frac{1}{8} & \frac{-1}{30} & \frac{-17}{120} \\ 0 & 0 & 1 & 0 & 0 & 0 & \frac{1}{15} & \frac{-2}{15} \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & \frac{1}{3} \end{bmatrix}$$

RESULTS CONTINUED…

In order to decrypt matrix B, multiply $A^{-1} \times$ B to get M.

So $A^{-1} \times B = M = \begin{bmatrix} 7 & 0 & 3 \\ 21 & 9 & 15 \\ 1 & 19 & 15 \\ 9 & 0 & 12 \end{bmatrix}$

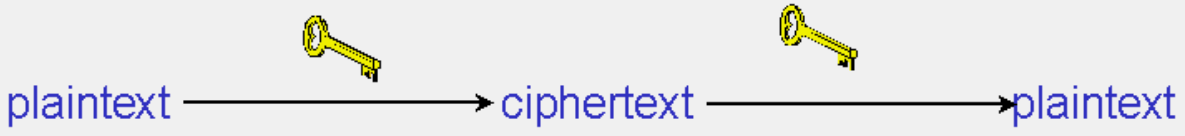
When changing the numbers of this matrix to the corresponding letters mentioned in the methods part, we get the message dedicated to our teacher:

RESULTS CONTINUED…

$$M = \begin{bmatrix} G & - & C \\ U & I & O \\ A & S & O \\ I & - & L \end{bmatrix}$$

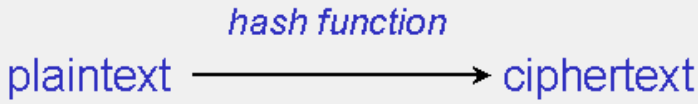
EXAMPLES:

An illustration:



A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.

B) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.



C) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the ciphertext.

The Secret Behind Cryptography

In Ancient Time

A scytale

Suppose the rod allows one to write 4 letters around in a circle and 5 letters down the side of it. The plaintext could be:

"Help me I am under attack“

To encrypt one simply writes across the leather...

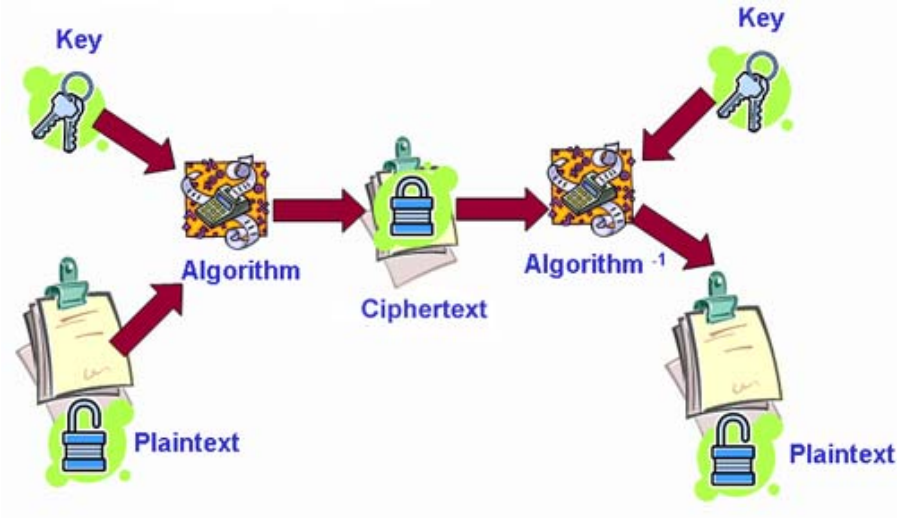
```
        |   |   |   |   |   |   |
        | H | E | L | P | M |   |
      __| E | I | A | M | U |__|
     |  | N | D | E | R | A |
     |  | T | T | A | C | K |
```

so the ciphertext becomes:

"**HENTEIDTLAEAPMRCMUAK**" after unwinding.

To decrypt all one must do is wrap the leather strip around the rod and read across. Every fifth letter will appear on the same line so the desired message can be read by the recipient.

In Modern Time

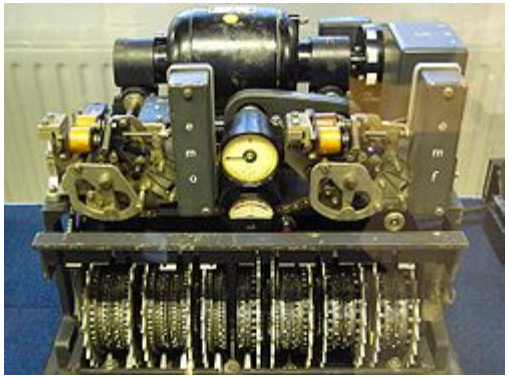


With the aid of modern technology.

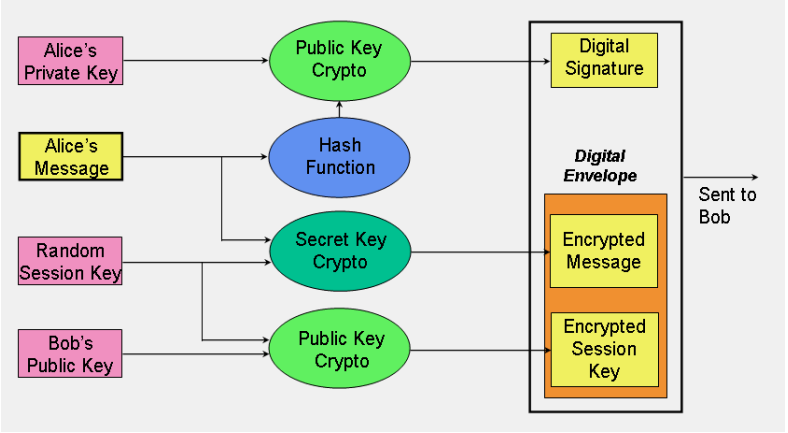
In war … and peace

16th-century book-shaped French cipher machine, with arms of Henri II of France

Credit card with smart-card capabilities. The 3-by-5-mm chip embedded in the card is shown, enlarged. Smart cards combine low cost and portability with the power to compute cryptographic algorithms.

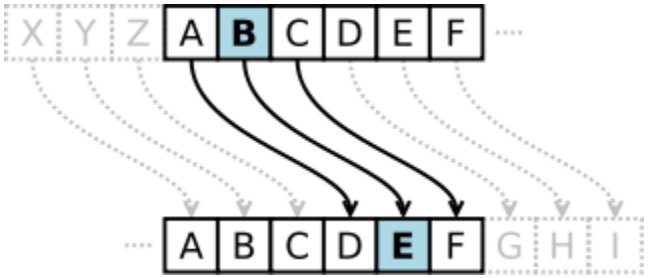


German Lorenz cipher machine, used in World War II to encrypt very-high-level general staff messages



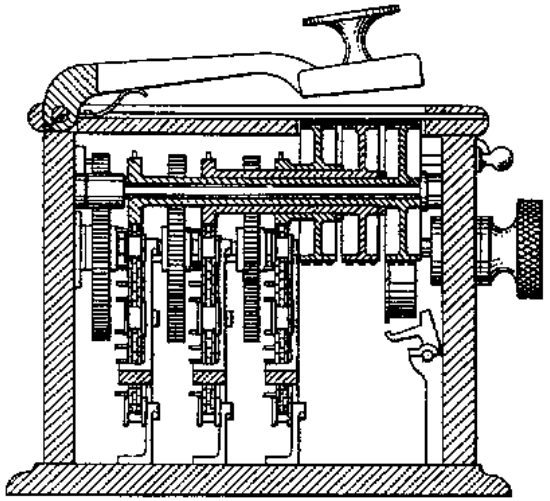
Message to send to a "secret" lover.

... and in memory

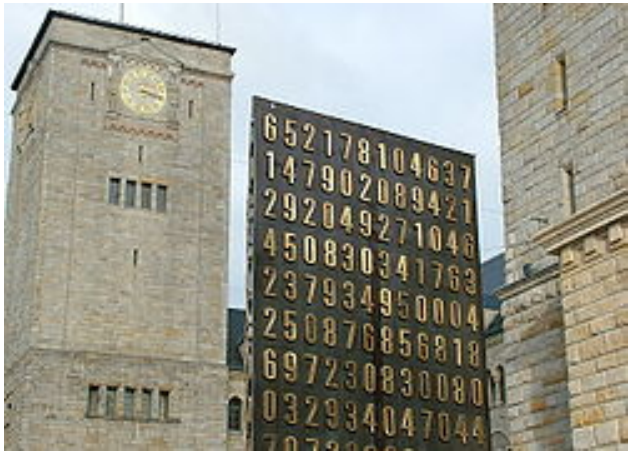


Caesercipher

The action of a Caesar cipher is to replace each plaintext letter with one a fixed number of places down the alphabet. This example is with a shift of three, so that a B in the plaintext becomes E in the ciphertext.



Hill's cipher of dimension 6 machine, invented by Lester S, Hill in 1929. It performed a 6 x 6 matrix multiplication modulo 26 using a system of gears and chains. Unfortunately, the machine didn't sell.



Poznań monument (*center*) to Polish cryptologists whose breaking of Germany's Enigma machine ciphers, beginning in 1932, altered the course of World War II

SUMMARY

1) We started by coming up with our own special code matrix A (Companies that encrypt their information have their own code matrix).
2) We use matrix A to encrypt any message (in this case matrix M) or information by multiplying A and M to yield an encrypted matrix B.
3) If we choose to decrypt matrix B, we must first find the inverse of A and multiply it with be to return to matrix M.

Conclusions

- In sum, cryptography offers many benefits and enhances the technological world that is continuously growing. As you have probably noticed, mathematical skills and knowledge about matrices are required to go through the process of encrypting information. The importance of linear algebra is portrayed through these benefits such as but not limited to, cryptography.

ACKNOWLEDGEMENTS

1) Thanks to Dr. Jen-Mei Chang!
2) L.S. Hill Cryptography in an Algebraic Alphabet. American Mathematical Monthly, 36 (1929), 306-312.
3) David C. Lay. Linear Algebra and Its Applications. Addison-Wesley, 3rd Edition, 2005.
4) Courtesy images from the following sites:

http://en.wikipedia.org/wiki/File:Smartcard3.png

http://en.wikipedia.org/wiki/File:Lorenz-SZ42-2.jpg

http://en.wikipedia.org/wiki/File:16th_century_French_cypher_machine_in_the_shape_of_a_book_with_arms_of_Henri_II.jpg

http://middleware.its.state.nc.us/middleware/Documentation/en_US/htm/csqzas00/csqzas000m.htm

http://en.wikipedia.org/wiki/File:Skytale.png

http://en.wikipedia.org/wiki/File:2008-09_Kaiserschloss_Kryptologen.JPG

http://en.wikipedia.org/wiki/Hill_cipher

http://en.wikipedia.org/wiki/File:Caesar3.svg