
A Brief History of Cryptography including Related Terms

*Crypto Background
Cryptography Zero*

*Ed Crowley
Spring 2010*

Topics



- Definitions
- Selected History
- Roots
- Hand Ciphers
- Machine Ciphers
- Computer Ciphers
- Related Terms

Necessity is the mother of invention, and computer networks are the mother of modern cryptography.

--R. Rivest

Secret Writing Ciphers and Codes

- Cryptography can be considered a branch of secret writing.
 - Like steganography, cryptography grew out of a need for confidentiality.
 - Cryptography creates ciphers
- Codes, in contrast to ciphers, are also a branch of secret writing.
 - Differ from ciphers in that codes work at the word level, while ciphers work at the character level.

What is Cryptology?

A mathematical science comprised of two branches of study (RFC 2828)

- Cryptography
 - Transforming data to
 - Render its meaning unintelligible (i.e., to hide its semantic content)
 - Prevent undetected alteration
 - Prevent unauthorized use
 - Cryptanalysis: Analysis of a cryptographic system to break or circumvent the protection that the system is designed to provide
 - Cryptanalyst is the natural antagonist of the cryptographer
-

Cryptosystems

- A cryptographic system (or cryptosystem)
 - is a set of algorithms together with the key management processes that support use of the algorithm in some application context
 - May also be called a scheme i.e. a digital signature scheme

RFC 2828

Classes

- Unkeyed
 - Cryptographic system that uses no secret parameter
- Secret key
 - Cryptographic system that uses secret parameters shared between the participating entities
- Public key
 - Cryptographic system that uses secret parameters not shared between the participating entities

Applied Cryptographic Services

- Data integrity
- Entity authentication
- Data origin authentication
- Access control
- Nonrepudiation
- Accountability
- Anonymity
- Pseudonymity

Security

- A cryptosystem is secure if a specified adversary cannot or is not able to solve a specified task

Two security notions

- If the adversary cannot solve the task, then one is in the realm of unconditional or information theoretic security (probability and/or information theory)
- If the adversary can in principle but is not able to solve the task, then one is in the realm of conditional or computational security (complexity theory)

Selected History



- 5th century BC, Cicero reported that secret writing saved the Greeks from the Persians.
- An Athenian invented steganography 4000 years ago
 - 400 BC, Spartans employed military cryptography in the form of a strip of papyrus or parchment wrapped around a wooden rod. (*Scytale cipher*)
- 49 BC, Julius Caesar used substitution ciphers.
- 9th century Baghdad, first recorded monoalphabetic cipher cryptanalysis.
 - All monoalphabetical ciphers can be cracked with frequency analysis (histogram)

Selected History

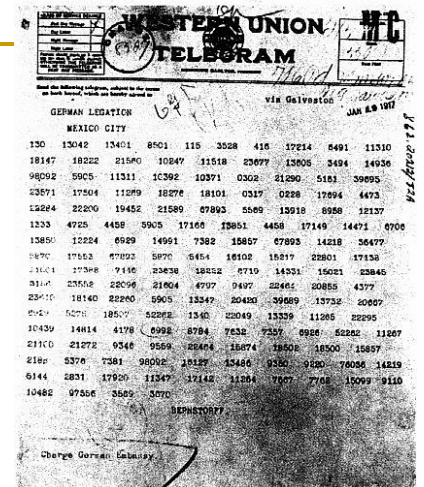
- Until 16th century, monoalphabetic ciphers continued to be widely used.
 - 16th century, polyalphabetic (Vigenere) cipher was popularized.
 - Though, Leon Battista Alberti is credited with the concept.
- During the Renaissance, cryptanalysis became a profession and gave rise to Black Chambers.
 - Black Chambers were groups of people who intercepted and read letters as well paid employees of governments including England, France, and Austria in the 1700s.
- 1790, Thomas Jefferson developed a mechanical encryption device

Jefferson Disk

- 1795, Thomas Jefferson invented the Jefferson disk cipher system
 - Used 26 wheels
 - Each with letters of alphabet arranged randomly around them.
- A century later, system reinvented by Commandant Etienne Bazeries.
 - Become known as Bazeries Cylinder.
 - System was also known as the M-94.
 - From 1923 until 1942, used by US Army.



Selected History



- 1883, Kerckhoff's Principle
 - A cryptosystem's security must not depend on keeping the algorithm secret.
 - All security depends only on the key.
 - Also known as Shannon's Maxim....
- 1917, Zimmerman Telegram
 - Encrypted German Telegram that offers Texas back to Mexico in return for Mexico's actions during war.
 - Contributed to U.S. entry in WWI

Zimmerman Telegram -- 1917

MAILED
October 1-8-18
London, State Dept.

*sent A. Eckhoff [unclear]
Oct 27, 1917*

TELEGRAM RECEIVED.

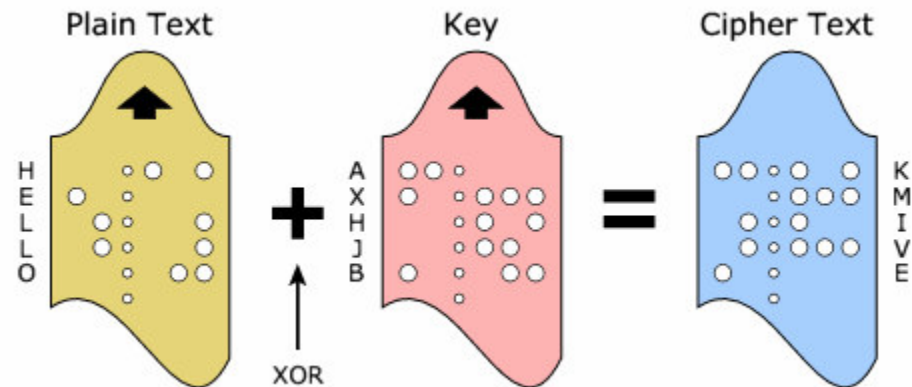
FROM 2nd from London # 5747.

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, ~~invite~~ ^{invite} Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that

Selected History

1919, Vernam stream cipher

- Stream cipher in which the plaintext is XORed with a random or pseudorandom stream of data the same length to generate the ciphertext.
 - For example, RC4 is a Vernam cipher that uses a pseudo-random number generator



Selected History

- 1925 (approx), One Time Pad
 - Only cryptographic methodology that, when implemented correctly can be proven to be unbreakable.*
 - Key management issues make it impossible to implement correctly.
 - Special case of Vernam stream cipher where key is truly random.
 - Key must only be used only once.
 - Not practical. Implementation requires compromise.
 - See Venona Project at NSA online museum

**1949 Claude Shannon*

Herbert Yardley and the American Black Chamber *(published 1931)*



Yardley considered Father of American Cryptography.
Headed MI 8 in NYC. (Part of Signal Corp.)
Among other accomplishments, MI 8, broke Japanese diplomatic codes
and furnished American negotiators with significant information during
1921-1922 Washington Naval Conference.

Selected History

- 1920, William F. Friedman published “The Index of Coincidence and Its Applications in Cryptography”.
 - Index of coincidence a statistical measure of text which distinguishes text encrypted with a monoalphabetic cipher and more complicated Vigenere methods (aka polyalphabetic ciphers.)
 - Considered by some to be the most important publication in modern cryptology to that time.
- Friedman coined several terms, including "cryptanalysis", meaning the study and practice of breaking codes and ciphers.
- Credited with running the team that broke the Purple machine as well as contributed to the SIGABA

Selected History

1933—1945, German Enigma

- ❑ Polyalphabetic substitution cipher machine.
- ❑ Cracked by a group led by the British at Bletchley Park
- Unix includes a substitution cipher ROT 13 that shifts the alphabet by 13 places.
 - ❑ `http://www.rot13.com/index.php`

1970, Feistel at IBM developed Lucifer.

- ❑ Later, evolved into DES.

1976, Diffie –Hellman--Merkle Public Key Encryption

1978, RSA Algorithm, by Rivest, Shamir, and Adleman

1973, Originally discovered by Clifford Cocks of GCHQ unclassified 1997

1991, PGP Phil Zimmerman

2000, AES wins NIST competition.

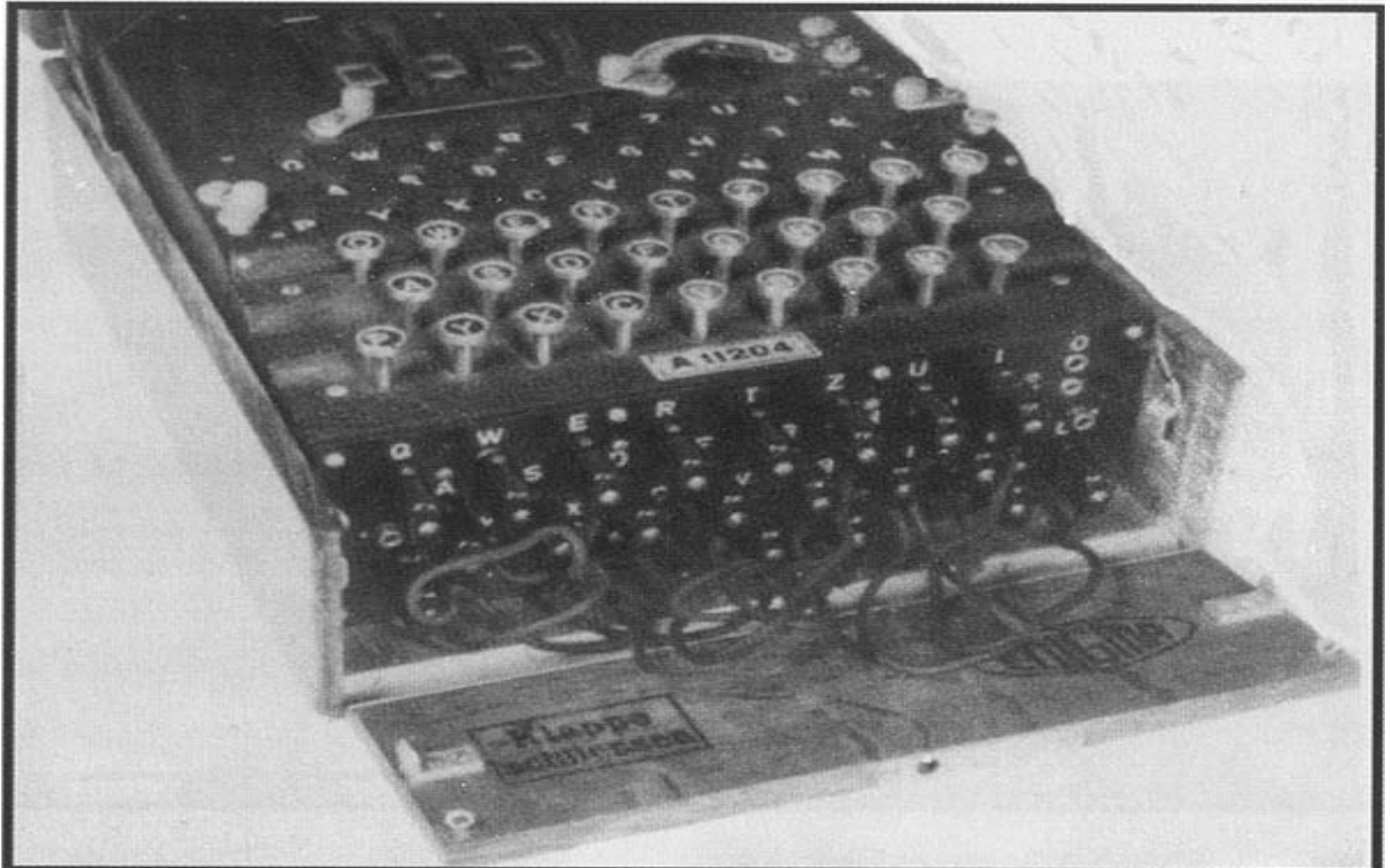
Cryptography Evolution

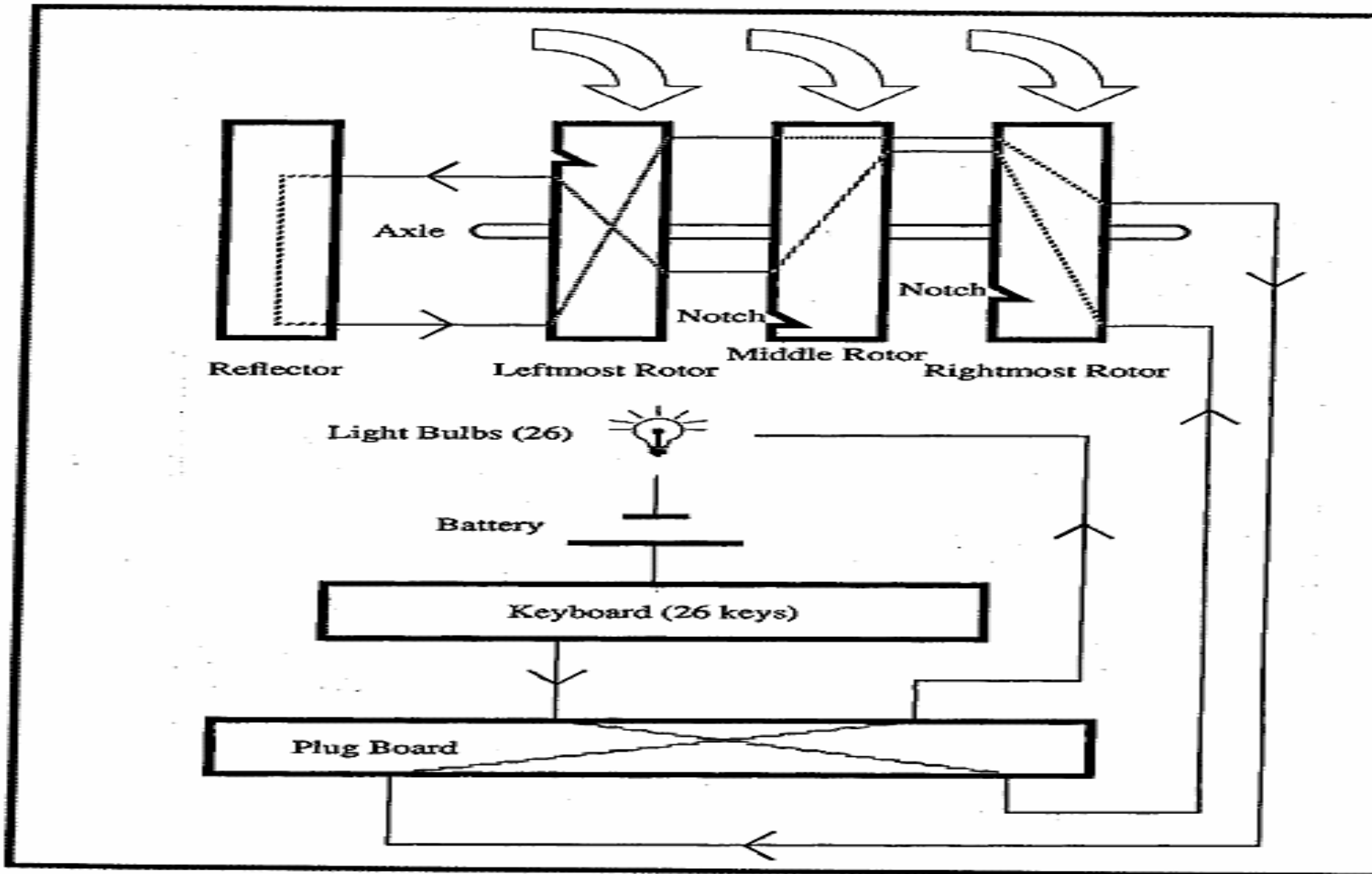
- Hand Ciphers
 - Monoalphabetic
 - Polyalphabetic – Vigenere Cipher
 - Utilize transposition and substitution aka confusion and diffusion
- Machine Ciphers
 - Engima
 - <http://ed-thelen.org/comp-hist/NSA-Comb.html>
 - Purple
 - Sigaba
- Computerized Ciphers and Cryptosystems
 - Symmetric
 - Asymmetric
 - Unkeyed or one way
 - Hybrid
- Quantum Future?

Machines

- Jefferson made the first rotary machine cipher (36 key)
- Later rotary machines included the German Engima and the American Sigaba
- Rather than rotors, Japanesse Purple Machine utilized stepper switches like those in automated telephone exchanges

Engima





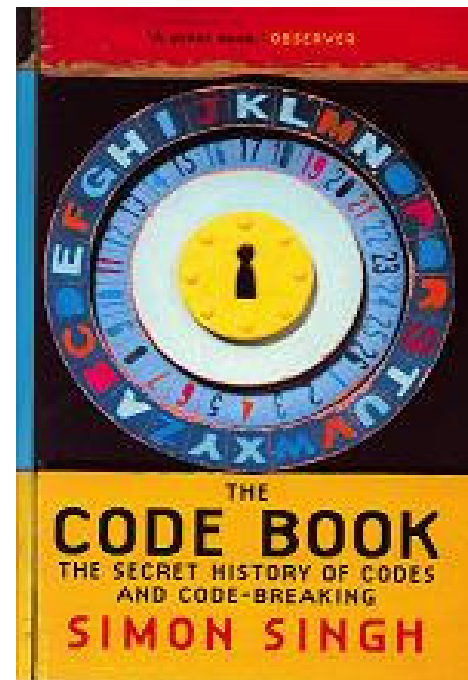
Internal wiring of Enigma showing one connection



Selected History

For a good historical presentation see: Simon Singh's: "The Code Book" :

Note that you can download an excellent Multimedia Cryptography CD from Singh's Crypto Corner.



http://www.simonsingh.net/Crypto_Corner.html

Selected Cryptographic Terms

- Algorithm
 - A well-defined procedure or sequence of steps used to produce a key stream or cipher text from plain text and vice versa. (*Orange Book*)
- Block Cipher
 - Obtained by segmenting plaintext into fixed size blocks and applying the identical encryption algorithm and key to each block. (*Contrast with stream cipher.*)
- Block Chaining
 - Parts of previous block are inserted into current block

Cryptographic Terms

- Cipher
 - A method that encrypts or disguises text.
- Clustering
 - Situation when a plain text message generates identical cipher text messages using the same transformation algorithm but with different keys.
- Codes
 - A cryptographic transformation that operates at the level of words or phrases.

Cryptographic Terms

- **Cryptanalysis**
 - The science of analyzing and breaking secure communication..
- **Ciphertext**
 - Plaintext that has been encrypted.
- **Decryption**
 - Changing ciphertext back to plaintext.
- **Key**
 - Sequence of bits and instructions that governs encryption and/or decryption.

Cryptographic Terms

- Keyspace
 - Range of values that can be used to construct a key.
- Key clustering
 - When a plaintext message generates identical ciphertext messages using the same transformation algorithm, but with different keys.
- Link Encryption
 - In the transmission chain, where each entity has keys in common with its two neighboring nodes.
- Plaintext
 - Data that can be read and understood without any special measures aka cleartext.
- Stream cipher
 - Message broken into characters or bits and enciphered with a key stream. (Contrast with block cipher.)

Cryptographic Terms

- Plaintext
 - Data that can be read and understood without any special measures aka cleartext.
- Stream cipher
 - Message broken into characters or bits and enciphered with a key stream. (Contrast with block cipher.)
- Passphrase
 - A sequence of words, or text, used to control access to a computer system, program or data.
 - Particularly applicable to systems that use the passphrase as an encryption key.

Selected Terms

- Stenography
 - Secret communications where the existence of the message is hidden.
- Work Function (factor)
 - Measure of difficulty in recovering plaintext from cipher text.
 - Measured by cost and/or time.
 - Another name for work factor is encryption method strength.

Questions?

References One:

<http://ed-thelen.org/comp-hist/NSA-Comb.html>

http://www.simonsingh.net/Crypto_Corner.html

<http://www.nsa.gov/museum/index.cfm>

<http://www-106.ibm.com/developerworks/library/s-pads.html>

<http://www.math.temple.edu/~renault/cryptology/affine.html>

References Two

https://www.isc2.org/cgi-bin/request_studyguide_form.cgi?AG=6042

<http://www.microsoft.com/resources/documentation/windows/2000/server/reskit/en-us/distsys/part2/dsgch14.msp>

<http://www.fas.org/irp/nsa/rainbow.htm>

Crypto FAQ

<http://www.spinstop.com/schlaflly/crypto/faq.htm>