A Brief History of Cryptography including Related Terms

Crypto Background

Ed Crowley

Fall '08

Topics

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

Secret Writing Ciphers and Codes

- Cryptography, like steganography, 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.

Selected History

- Fifth 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.
  - Frequency analysis vulnerability

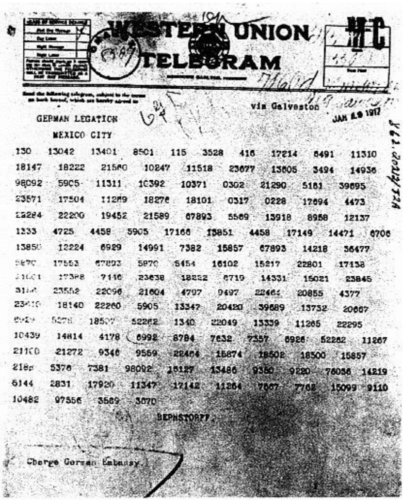
Selected History

- 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



WESTERN UNION TELEGRAM

via Galveston JAN 19 1917

GERMAN LEGATION
MEXICO CITY

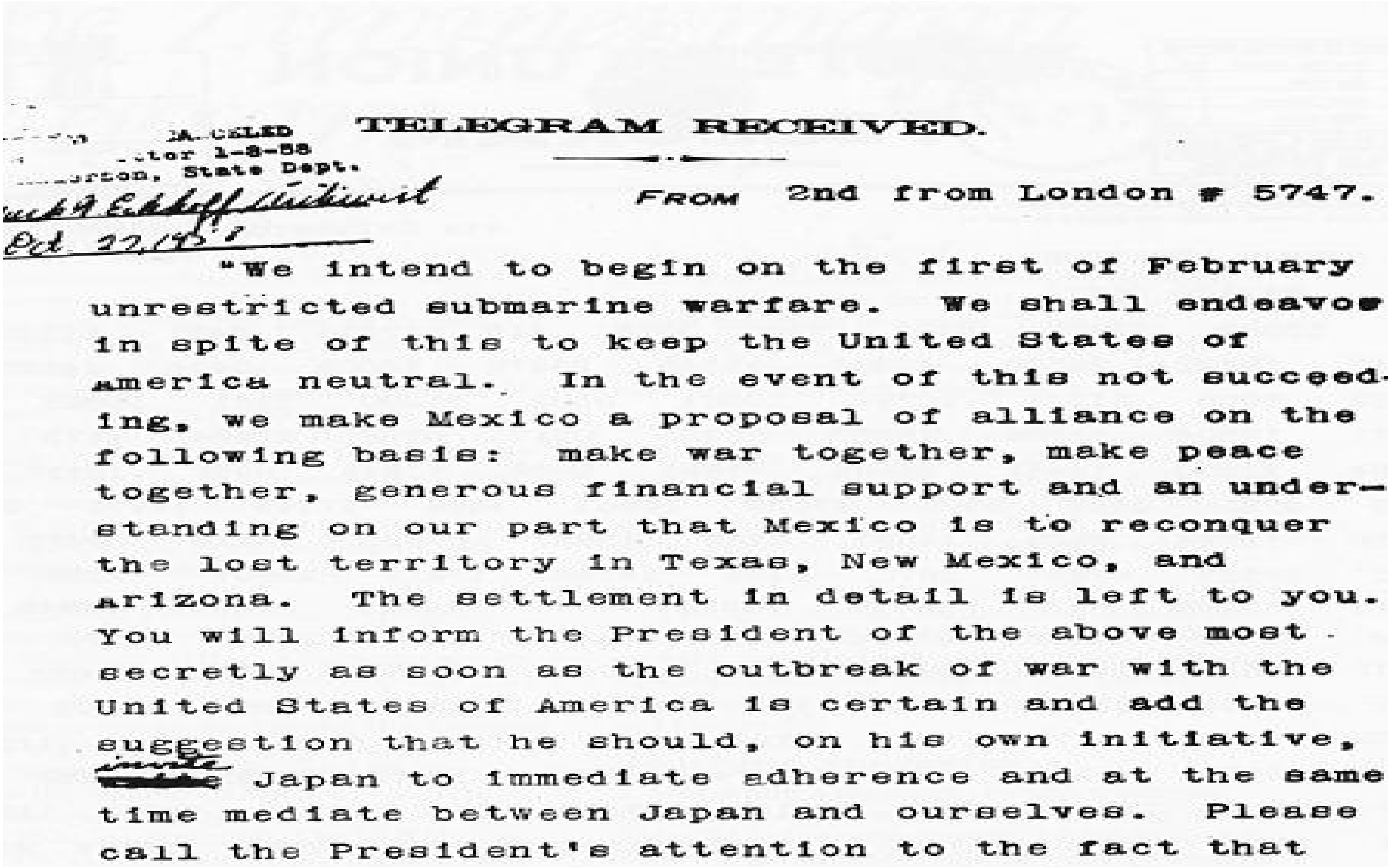
```
130    13042  13401  8501   115    3528   416    17214  6491   11310
18147  18222  21560  10247  11518  23677  13605  3494   14936
98092  5905   11311  10392  10371  0302   21290  5161   39695
23571  17504  11269  18276  18101  0317   0228   17694  4473
22284  22200  19452  21589  67893  5569   13918  8958   12137
1333   4725   4458   5905   17166  13851  4458   17149  14471  6706
13850  12224  6929   14991  7382   15857  67893  14218  36477
5870   17553  67893  5870   5454   16102  15217  22801  17138
21001  17388  7446   23638  18222  6719   14331  15021  23845
3156   23552  22096  21604  4797   9497   22464  20855  4377
23610  18140  22260  5905   13347  20420  39689  13732  20667
6929   5275   18507  52262  1340   22049  13339  11265  22295
10439  14814  4178   6992   8784   7632   7357   6926   52262  11267
21100  21272  9346   9559   22464  15874  18502  18500  15857
2188   5376   7381   98092  16127  13486  9350   9220   76036  14219
5144   2831   17920  11347  17142  11264  7667   7762   15099  9110
10482  97556  3569   3670
```

BERNSTORFF.

Charge German Embassy.

- 1883, Kerckhoff's Principle
  - A cryptosystem's security of must not depend on keeping the algorithm secret.
    - All security depends only on the key.
- 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



..A..CELED
..tor 1-8-58
..erson, State Dept.
..ck A Eckhoff Archivist
Oct. 22, 1957

TELEGRAM RECEIVED.

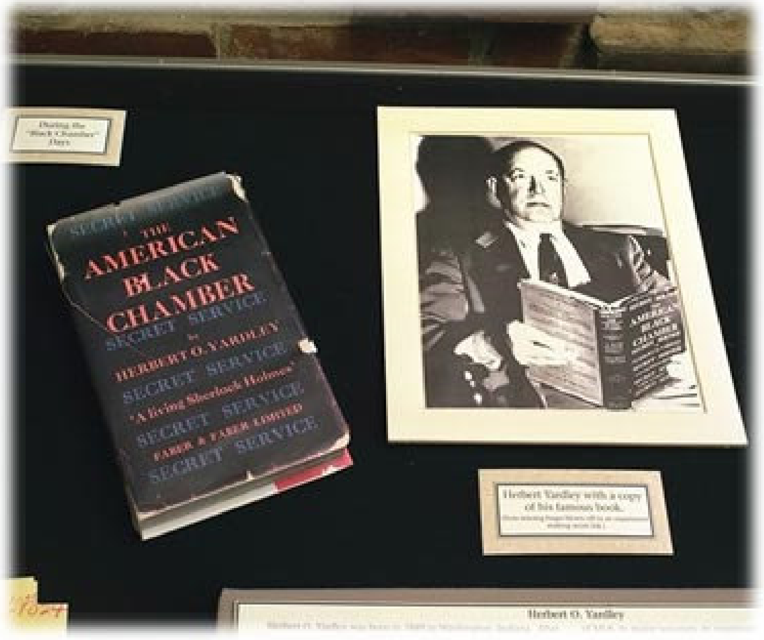
FROM 2nd from London # 5747.

"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 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

- 1917, 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 the same length as message.
    - Key must only be used only once.
    - Key's components must be truly random
      - No periodicity or predictability.
    - Not practical. Implementation requires compromise.
      - See Venona Project at NSA online musuem

Herbert Yardley and the American Black Chamber



Published 1920

Yardley considered Father of American Cryptography.

Among other accomplishments, broke Japanese diplomatic codes and furnished American negotiators with significant information during 1921-1922 Washington Naval Conference.

Selected History

- 1920, William Frederick Friedman published “The Index of Coincidence and Its Applications in Cryptography”.
  - Index of coincidence is a statistical measure of text which distinguishes text encrypted with a simple substitution cipher (aka 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.

Selected History

- 1933—1945, German Enigma
  - Polyalphabetic substitution cipher machine.
  - Cracked bya group led by the British at Benchly 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
- 1991, PGP Phil Zimmerman
- 2000, AES wins NIST competition.

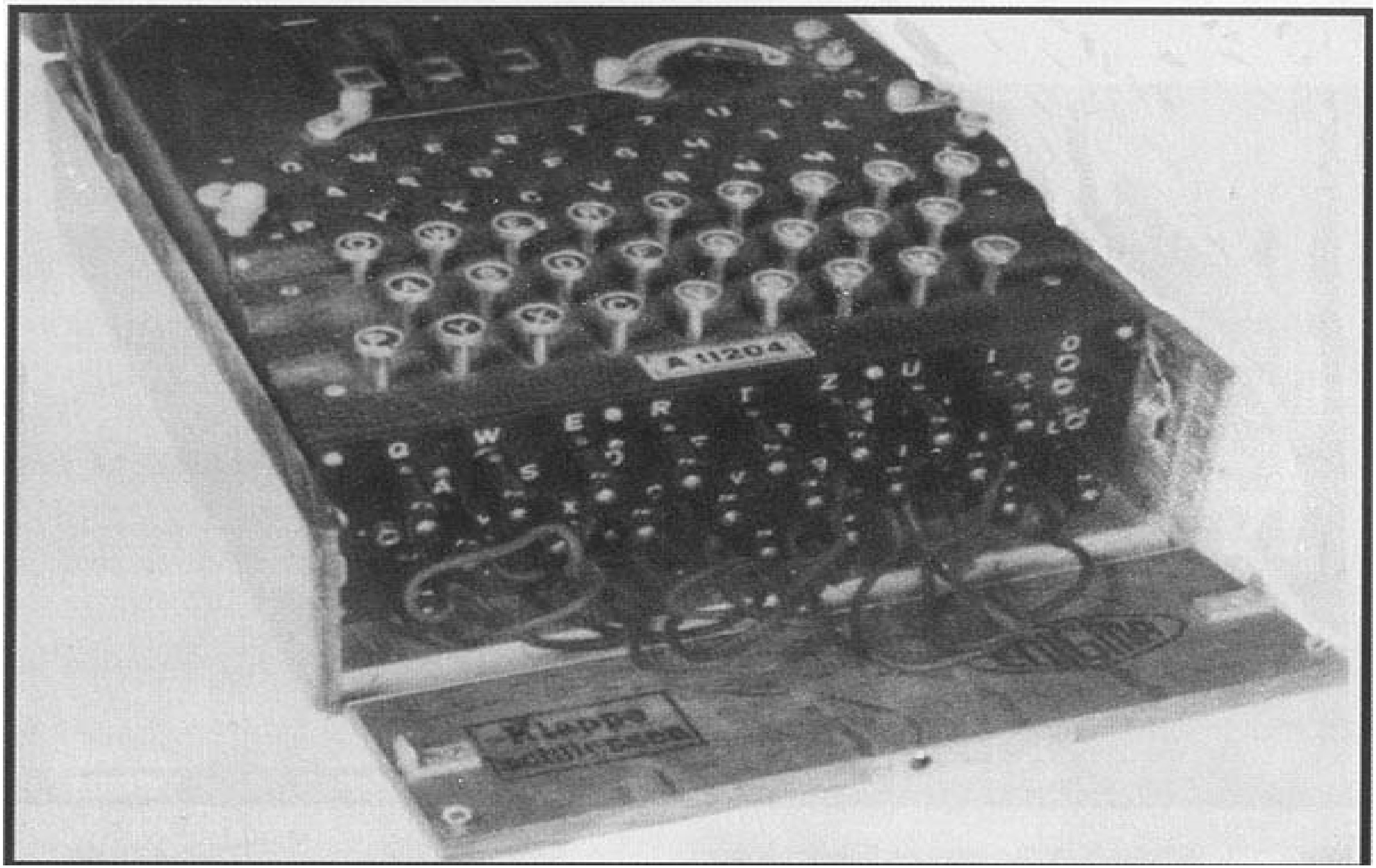
Cryptography Evolution

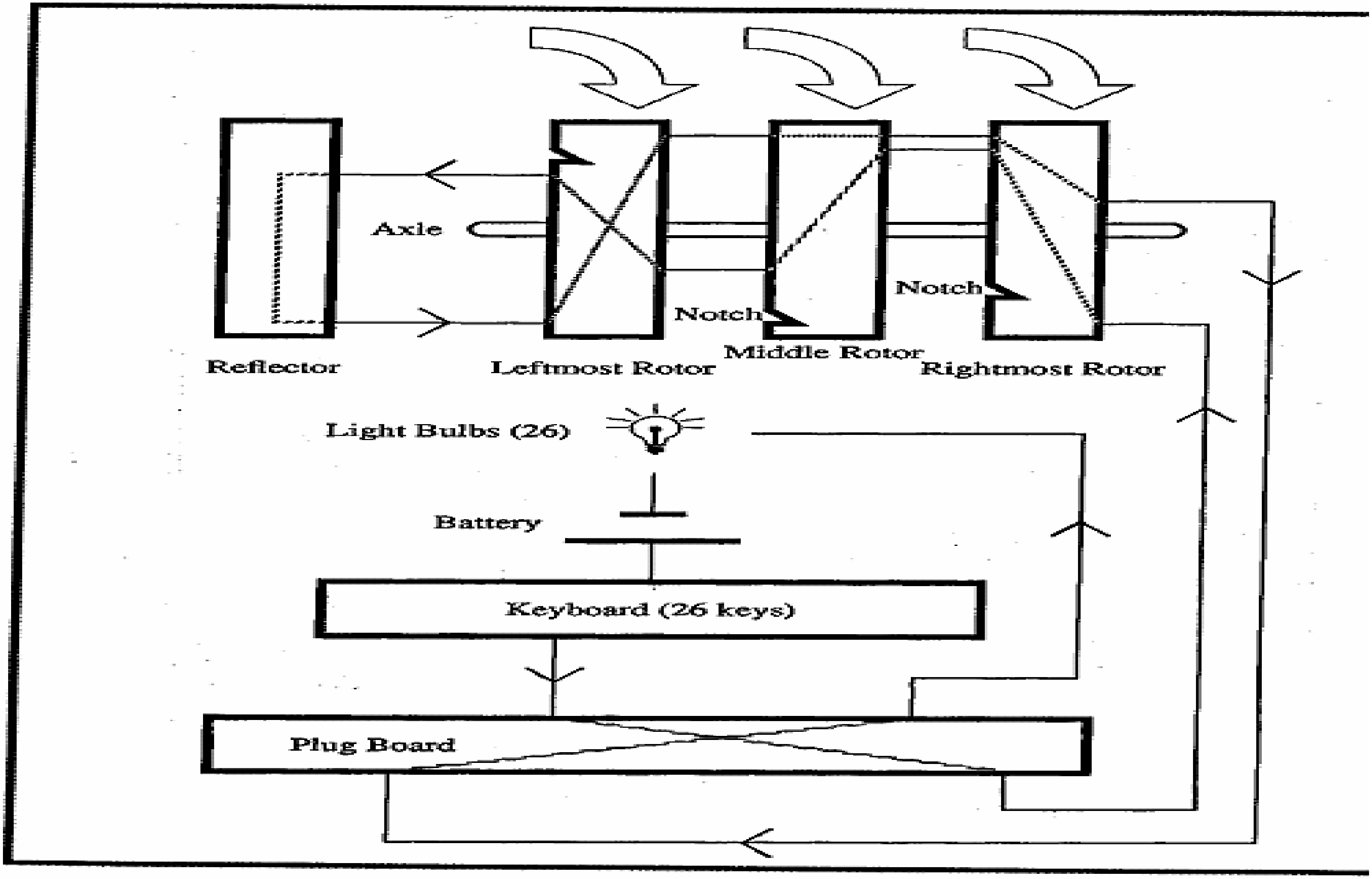
- Hand Ciphers
  - Monoalphabetic
  - Polyalphabetic – Vigenere Cipher
  - Utilize transposition and substitution aka confusion and diffusion
- Machine Ciphers
  - Engima
    - http://ed-thelen.org/comp-hist/NSA-Comb.html
  - Purple
  - Sigaba
- Computerized Ciphers and Cryptosystems
  - Symmetric
 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

Machines

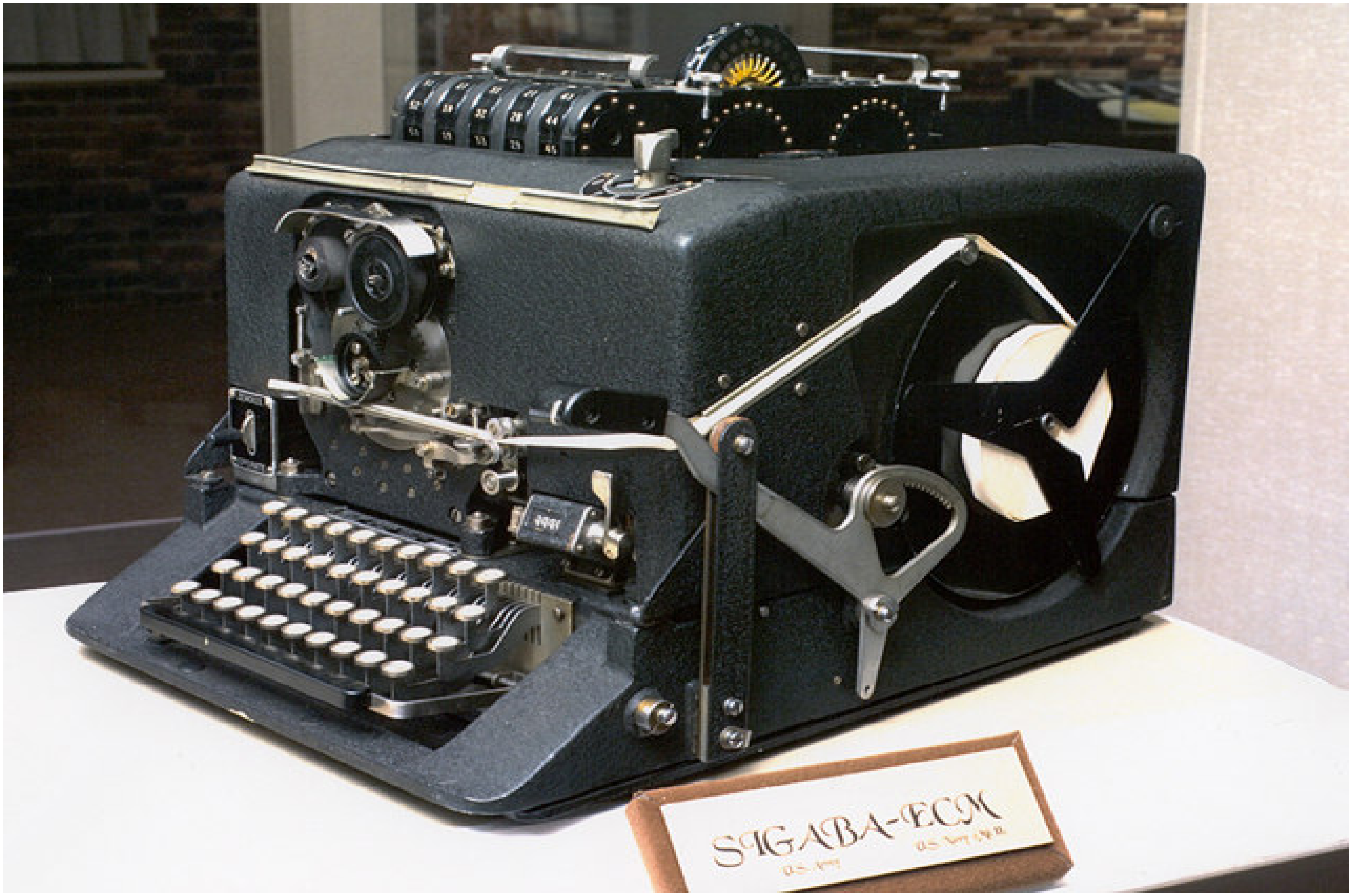
- Jefferson made the first rotary machine cipher (Vigenere 36 key)
- Later rotary machines included the German Engima and the American Sigaba
- Japanesse Purple which utilized stepper switches like those in automated telephone exchanges rather than rotors

Engima





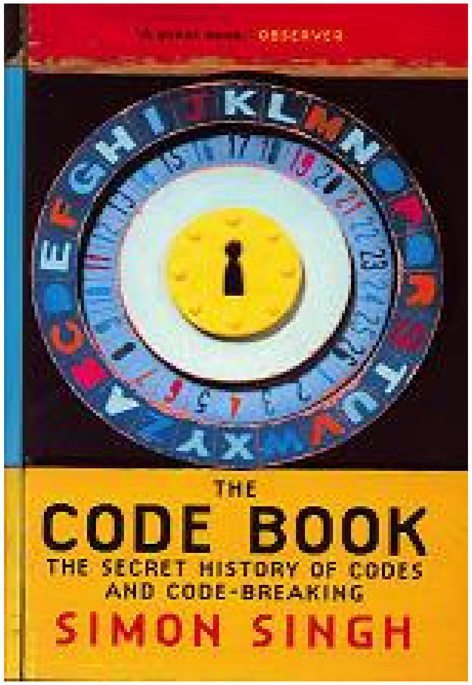
Internal wiring of Enigma showing one connection



SIGABA-ECM

Selected History

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



Note that you can download
an excellent 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 modes.
- 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.mspx

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

Crypto FAQ

http://www.spinstop.com/schlafly/crypto/faq.htm

Appendix

- Who am I?

Who am I?

- Developed four, three credit hour, graduate level UH Security Courses
- Past Security Presentations at: University of Indiana in Pennsylvania’s Network Security Workshop, Infragard, ISACA, ACM SIGITE, and American Association for Engineering Education
- Created/presented workshops at the New Jersey Institute of Technology and Sam Houston State University.
- Earned CISSP, NSA IAM & IEM, Security Certifications
  - Usual certifications from usual suspects (Cisco, CompTIA, Novell, and Microsoft).
- Former Network Admin and IS Director
- Graduate Military Police Academy
  - USARPAC German Shepard Sentry Dog School
  - Secret Clearance (expired)