CRYPTO BASICS

PREPARED BY:

DR. MUHAMMAD IQBAL HOSSAIN

ASSOCIATE PROFESSOR

DEPARTMENT OF CSE, BRAC UNIVERSITY

APPENDIX

HOW TO SPEAK CRYPTO

SUBSTITUTION CIPHER

TRANSPOSITION CIPHER

ONE-TIME PAD

CODEBOOK CIPHER

CRYPTO HISTORY

TAXONOMY

CRYPTO

- Cryptology — The art and science of making and breaking "secret codes"
- Cryptography — making "secret codes"
- Cryptanalysis — breaking "secret codes"
- Crypto — all of the above (and more)

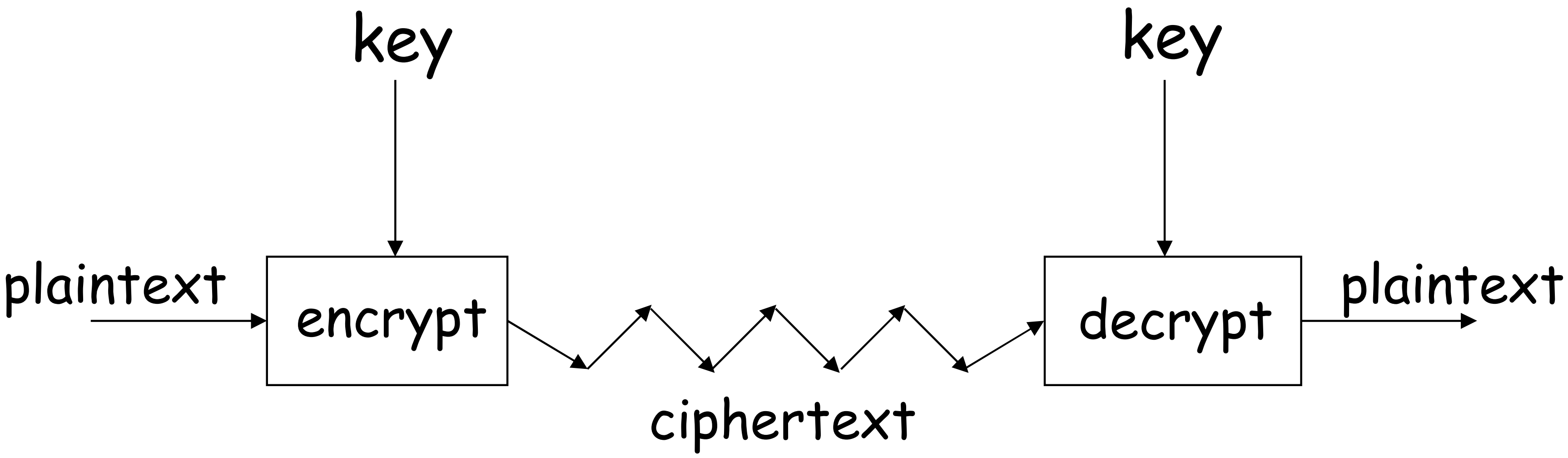
HOW TO SPEAK CRYPTO

- A cipher or cryptosystem is used to encrypt the plaintext
- The result of encryption is ciphertext
- We decrypt ciphertext to recover plaintext
- A key is used to configure a cryptosystem
- A symmetric key cryptosystem uses the same key to encrypt as to decrypt
- A public key cryptosystem uses a public key to encrypt and a private key to decrypt (sign)

CRYPTO

- Basis assumption
  - The system is completely known to the attacker
  - Only the key is secret
- Also known as Kerckhoffs Principle
  - Crypto algorithms are not secret
- Why do we make this assumption?
  - Experience has shown that secret algorithms are weak when exposed
  - Secret algorithms never remain secret
  - Better to find weaknesses beforehand

CRYPTO AS BLACK BOX



A generic use of crypto

CLASSIC CRYPTO

SIMPLE SUBSTITUTION

- Plaintext: fourscoreandsevenyearsago
- Key:

Plaintext Ciphertext

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- Ciphertext: IRXUVFRUHDAGVHYHABHDUVDIR
- Shift by 3 is "Caesar's cipher"

CEASAR’S CIPHER DECRYPTION

- Suppose we know a Ceasar’s cipher is being used
- Ciphertext:

VSRQJHEREVTXDUHSDQWU

Plaintext Ciphertext

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

○ Plaintext: spongebobsquarepants

NOT-SO-SIMPLE SUBSTITUTION

- Shift by n for some $n \in \{0, 1, 2, \cdots, 25\}$
- Then key is n
- Example: key = 7

Plaintext Ciphertext

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G

- End of segment 1

CRYPTANALYSIS I: TRY THEM ALL

- Given
  - A simple substitution (shift by n) is used
  - But the key is unknown
  - Given ciphertext: meqefscerhcsyeviekmvp
- How to find the key?
- Exhaustive key search
  - Only 26 possible keys — try them all!
  - Solution: key = 4 IAMABOYANDYOUAREAGIRL

EVEN-LESS-SIMPLE SUBSTITUTION

- Key is some permutation of letters
- Need not be a shift
- For example

Plaintext Ciphertext

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
J	I	C	A	X	S	E	Y	V	D	K	W	B	Q	T	Z	R	H	F	M	P	N	U	L	G	O

- Then 26! > 2^{88} possible keys!
- Dominates the art of secret writing throughout the first millennium

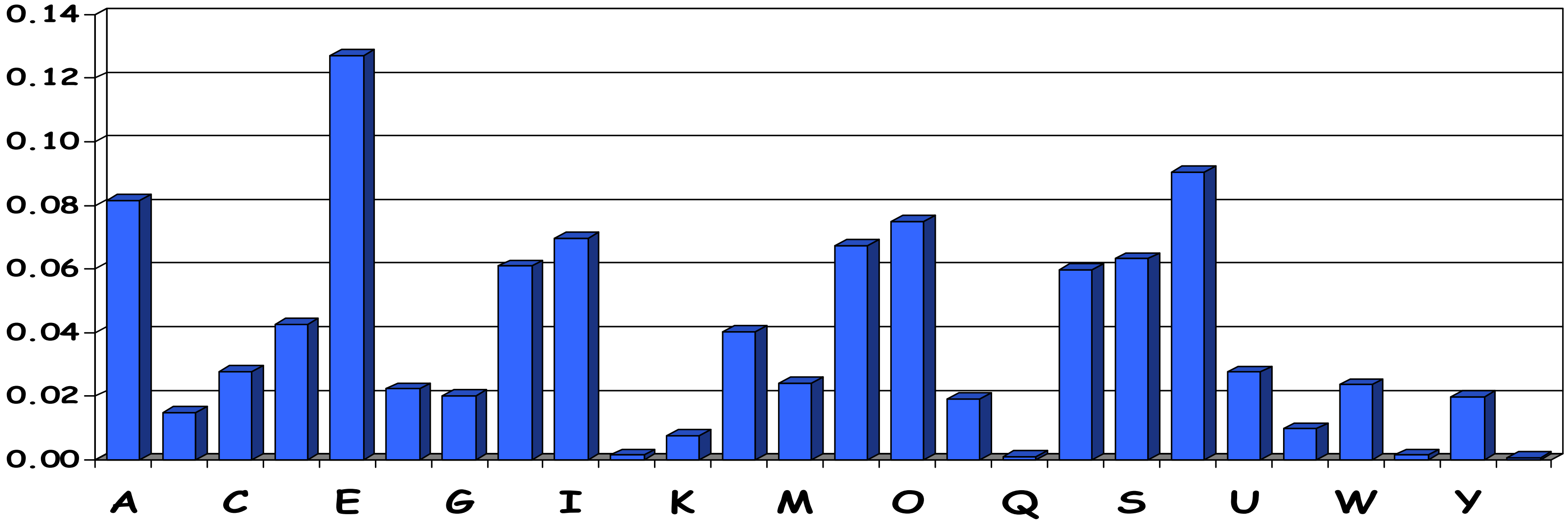
CRYPTANALYSIS II: BE CLEVER

- We know that a simple substitution is used
- But not necessarily a shift by *n*
- Can we find the key given ciphertext:

```
PBFPVYFBQXZTYFPBFEQJHDXXQVAPTPQJKTOYQWIPBVWLXTOXBTFXQWAXBVCXQWAXFQJVW
LEQNTOZQGGQLFXQWAKVWLXQWAEBIPBFXFQVXGTVJVWLBTPQWAEBFPBFHCVLXBQUFEVWLX
GDPEQVPQGVPPBFTIXPFHXZHVFAGFOTHFEFBQUFTDHZBQPOTHXTYFTODXQHFTDPTOGHFQP
BQWAQJJTODXQHFOQPWTBDHHIXQVAPBFZQHCFWPFHPBFIPBQWKFABVYYDZBOTHPBQPQJTQ
OTOGHFQAPBFEQJHDXXQVAVXEBQPEFZBVFOJIWFFACFCCFHQWAUVWFLQHGFXVAFXQHFUFH
ILTTAVWAFFAWTEVOITDHFHFQAITIXPFHXAFQHEFZQWGFLVWPTOFFA
```

CRYPTANALYSIS II

- Can’t try all 2^{88} simple substitution keys
- Can we be more clever?
- English letter frequency counts…



CRYPTANALYSIS II

- Ciphertext:

```
PBFPVYFBQXZTYFPBFEQJHDXXQVAPTPQJKTOYQWIPBVWLXTOXBTFXQWAXBVCXQWAXFQJVWLEQNTOZQG
GQLFXQWAKVWLXQWAEBIPBFXFQVXGTVJVWLBTPQWAEBFPBFHCVLXBQUFEVWLXGDPEQVPQGVPPBFTIXP
FHXZHVFAGFOTHFEFBQUFTDHZBQPOTHXTYFTODXQHFTDPTOGHFQPBQWAQJJTODXQHFOQPWTBDHHIXQV
APBFZQHCFWPFHPBFIPBQWKFABVYYDZBOTHPBQPQJTQOTOGHFQAPBFEQJHDXXQVAVXEBQPEFZBVFOJI
WFFACFCCFHQWAUVWFLQHGFXVAFXQHFUFHILTTAVWAFFAWTEVOITDHFHFQAITIXPFHXAFQHEFZQWGFL
VWPTOFFA
```

- Decrypt this message using info below

Ciphertext frequency counts:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
21	26	6	10	12	51	10	25	10	9	3	10	0	1	15	28	42	0	0	27	4	24	22	28	6	8

FREQUENCY ANALYSIS HISTRORY

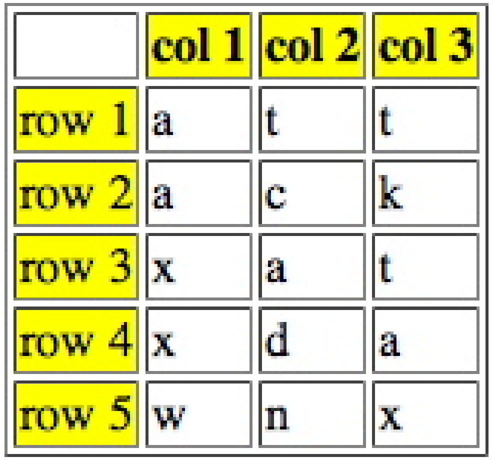
- Discovered by the Arabs
  - Earliest known description of frequency analysis is in a book by the 9-century scientist al-Kindi
- Rediscovered or introduced from the Arabs in Europe during the Renaissance
- Frequency analysis made substitution cipher inscure.

CRYPTANALYSIS: TERMINOLOGY

- Cryptosystem is secure if best know attack is to try all keys
- Cryptosystem is insecure if any shortcut attack is known
- By this definition, an insecure system might be harder to break than a secure system!

DOUBLE TRANSPOSITION

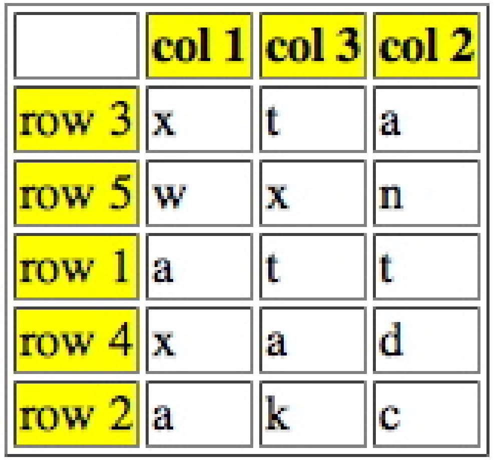
- Plaintext: attackxatxdawn



	col 1	col 2	col 3
row 1	a	t	t
row 2	a	c	k
row 3	x	a	t
row 4	x	d	a
row 5	w	n	x

Permute rows and columns

⇒



	col 1	col 3	col 2
row 3	x	t	a
row 5	w	x	n
row 1	a	t	t
row 4	x	a	d
row 2	a	k	c

- Ciphertext: xtawxnattxadakc
- Key: matrix size and permutations (3,5,1,4,2) and (1,3,2)

ONE-TIME PAD ENCRYPTION

e=000 h=001 i=010 k=011 l=100 r=101 s=110 t=111

Encryption: Plaintext ⊕ Key = Ciphertext

P	h	e	i	l	h	i	t	l	e	r
	001	000	010	100	001	010	111	100	000	101
K	111	101	110	101	111	100	000	101	110	000
C	110	101	100	001	110	110	111	001	110	101
	s	r	l	h	s	s	t	h	s	r

ONE-TIME PAD DECRYPTION

e=000 h=001 i=010 k=011 l=100 r=101
s=110 t=111

Decryption: Ciphertext ⊕ Key = Plaintext

C	s	r	l	h	s	s	t	h	s	r
	110	101	100	001	110	110	111	001	110	101
K	**111**	**101**	**110**	**101**	**111**	**100**	**000**	**101**	**110**	**000**
P	001	000	010	100	001	010	111	100	000	101
	h	e	i	l	h	i	t	l	e	r

ONE-TIME PAD

Double agent claims sender used "**key**":

C	s	r	l	h	s	s	t	h	s	r
	110	101	100	001	110	110	111	001	110	101
K	101	111	000	101	111	100	000	101	110	000
P	011	010	100	100	001	010	111	100	000	101
	k	i	l	l	h	i	t	l	e	r

e=000 h=001 i=010 k=011 l=100 r=101 s=110 t=111

ONE-TIME PAD

Sender is captured and claims the key is:

C	s	r	l	h	s	s	t	h	s	r
	110	101	100	001	110	110	111	001	110	101
K	111	101	000	011	101	110	001	011	101	101
P	001	000	100	010	011	000	110	010	011	000
	h	e	l	i	k	e	s	i	k	e

e=000 h=001 i=010 k=011 l=100 r=101 s=110 t=111

ONE-TIME PAD SUMMARY

- Provably secure, when used correctly
  - Ciphertext provides no info about plaintext
  - All plaintexts are equally likely
  - Pad must be random, used only once
  - Pad is known only by sender and receiver
  - Pad is same size as message
  - No assurance of message integrity
- Why not distribute message(plaintext) the same way as the pad(key)???

REAL-WORLD ONE-TIME PAD

- Project VENONA
  - Soviet spy messages from U.S. in 1940’s
  - Nuclear espionage, etc.
  - Thousands of messaged
- Spy carried one-time pad into U.S.
- Spy used pad to encrypt secret messages
- Repeats within the “one-time” pads made cryptanalysis possible

VENONA DECRYPT (1944)

[C% Ruth] learned that her husband [v] was called up by the army but he was not sent to the front. He is a mechanical engineer and is now working at the ENORMOUS [ENORMOZ] [vi] plant in SANTA FE, New Mexico. [45 groups unrecoverable]

detain VOLOK [vii] who is working in a plant on ENORMOUS. He is a FELLOWCOUNTRYMAN [ZEMLYaK] [viii]. Yesterday he learned that they had dismissed him from his work. His active work in progressive organizations in the past was cause of his dismissal. In the FELLOWCOUNTRYMAN line LIBERAL is in touch with CHESTER [ix]. They meet once a month for the payment of dues. CHESTER is interested in whether we are satisfied with the collaboration and whether there are not any misunderstandings. He does not inquire about specific items of work [KONKRETNAYa RABOTA]. In as much as CHESTER knows about the role of LIBERAL's group we beg consent to ask C. through LIBERAL about leads from among people who are working on ENOURMOUS and in other technical fields.

- "Ruth" == Ruth Greenglass
- "Liberal" == Julius Rosenberg
- "Enormous" == the atomic bomb

CODEBOOK

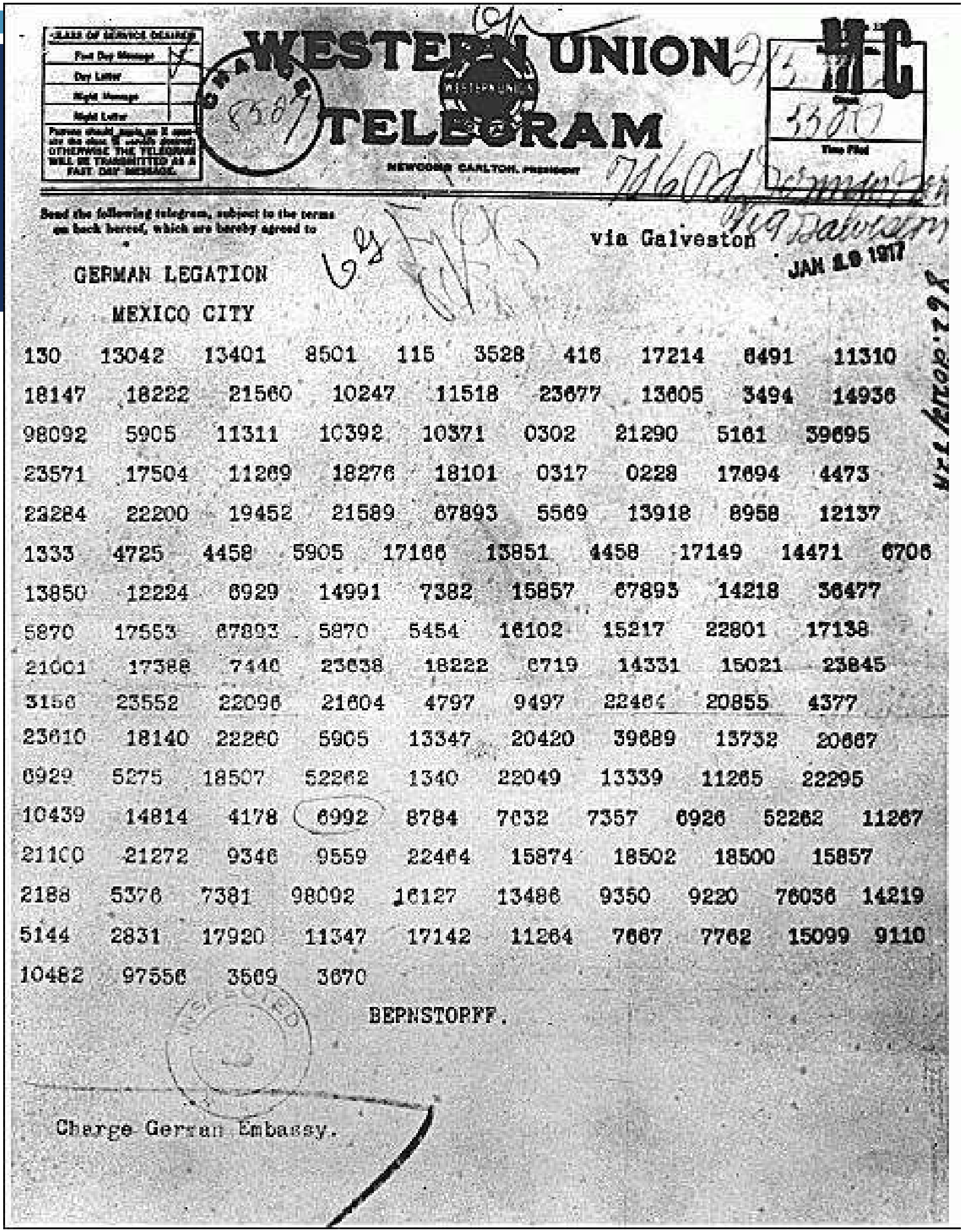
- Literally, a book filled with "codewords"
- Zimmerman Telegram encrypted via codebook

Februar	13605
fest	13732
finanzielle	13850
folgender	13918
Frieden	17142
Friedenschluss	17149
:	:

- Modern block ciphers are codebooks!
- More on this later…

ZIMMERMAN TELEGRAM

- One of most famous codebook ciphers ever
- Led to US entry in WWI
- Ciphertext shown here…



CLASS OF SERVICE DESIRED
Fast Day Message ☒
Day Letter
Night Message
Night Letter
Patrons should mark an X opposite the class of service desired; OTHERWISE THE TELEGRAM WILL BE TRANSMITTED AS A FAST DAY MESSAGE.

WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Check 3300

Time Filed

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

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

23284 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

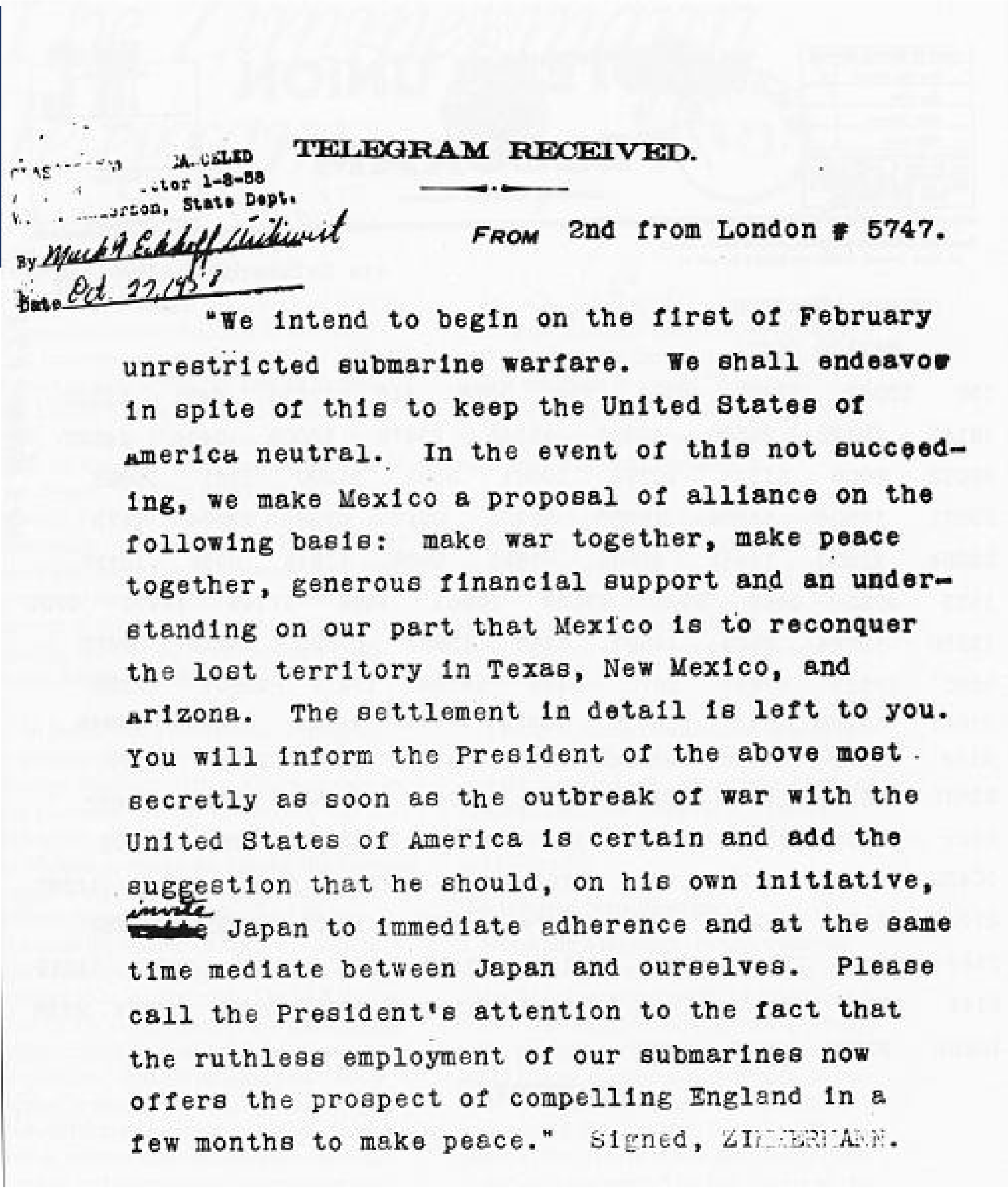
10482 97556 3569 3670

BERNSTORFF.

Charge German Embassy.

ZIMMERMAN TELEGRAM DECRYPTED

- British had recovered partial codebook
- Able to fill in missing parts



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

TELEGRAM RECEIVED.

FROM 2nd from London # 5747.

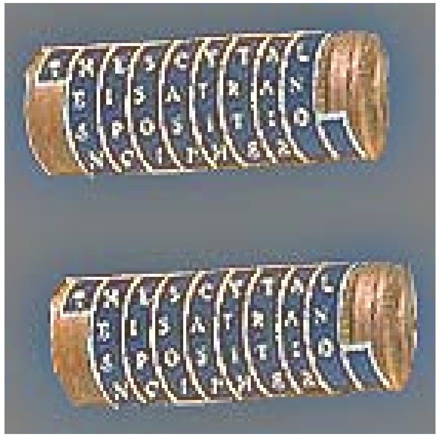
"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous 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, ~~[illegible]~~ 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 the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIMMERMANN.

- End of segment 2

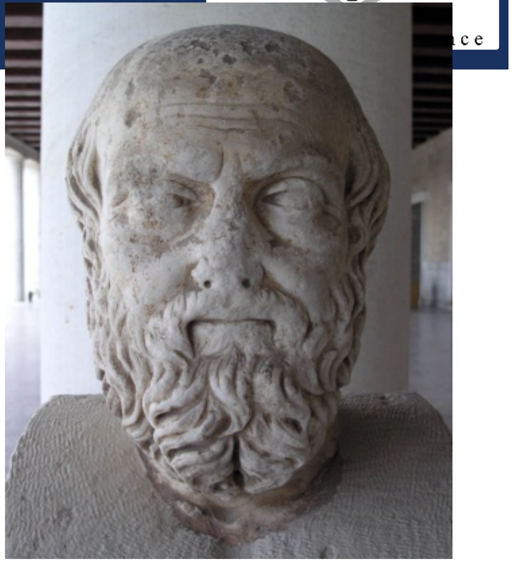
MORDERN CRYPTO HISTORY

TIMELINE OF CRYPTOGRAPHY

- Crypto timeline
  - Answers.com
  - Wikipedia
- BCE
  - 400 – Spartan use of scytale
    Transposition cipher



TIMELINE OF CRYPTOGRAPHY



- BCE
  - 400 - Herodotus: steganography
    - Shaved slave' s head (tattoo on shaved head)
    - Wrote message on head
    - Let hair grow back
    - Send slave to deliver message
    - Shave slave' s head to expose message (warning of Persian invasion)
    - Historically, Steganography has been used more than cryptography!
  - 100-1 CE - Caeser cipher. Substitution cipher

TIMELINE OF CRYPTOGRAPHY

- 1-1799 CE
  - 1000 – Frequency analysis: leading to techniques for breaking monoalphabetic substitution ciphers
  - 1553 – Vigenère cipher (invented by Belaso)
    - Plaintext: ATTACKATDAWN
      Key: LEMONLEMONLE
      Ciphertext: LXFOPVEFRNHR
  - 1645 – Wilkins' *Mercury* (English book on cryptology)

C.S.A.
S.S.
THE CONFEDERATE CIPHER DISK
The Confederate cipher disk was made of brass. Only two and one-quarter inches in diameter, it was small enough to easily fit into a vest pocket. The device consisted of two disks with the smaller inner disk revolving on a central pivot. Each disk had the alphabet (reading left to right) imprinted around its circumference. The red letters SS are thought to stand for Secret Service. Only five original examples are known to exist.

TIMELINE OF CRYPTOGRAPHY

- 1800-1899
  - 1835 - Samuel Morse develops the Morse code
  - 1854 - Wheatstone invents Playfair cipher
  - 1854 - Babbage's method for breaking polyalphabetic ciphers (pub 1863 by Kasiski)
  - 1883 - Auguste Kerckhoffs' *La Cryptographie militare* published, containing his celebrated laws of cryptography
  - 1885 - Beale ciphers published

TIMELINE OF CRYPTOGRAPHY

- 1900-1949
  - 1917 - Gilbert Vernam develops first practical implementation of a teletype cipher, now known as a stream cipher and, later, with Joseph Mauborgne the one-time pad
  - 1917 - Zimmermann telegram intercepted and decrypted, advancing U.S. entry into World War I
  - c. 1932 - first break of German Army Enigma by Marian Rejewski in Poland
  - 1929 - U.S. Secretary of State Henry L. Stimson shuts down State Department cryptanalysis "Black Chamber", saying "Gentlemen do not read each other's mail. "

TIMELINE OF CRYPTOGRAPHY

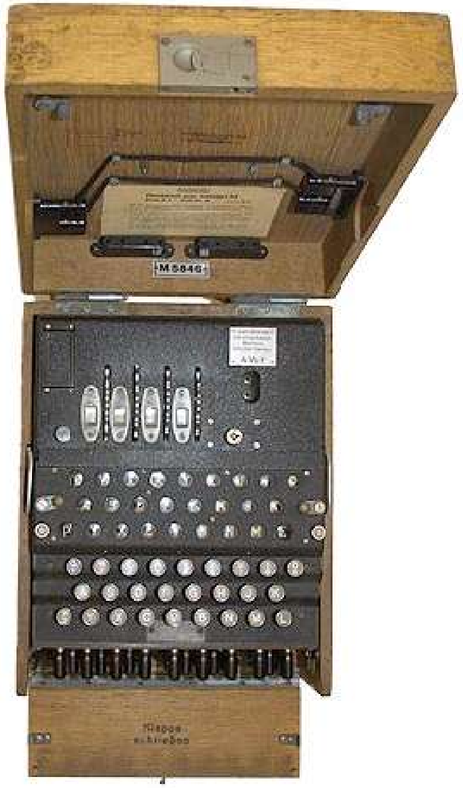
- 1900-1949
  - 1940 – break of Japan's PURPLE machine cipher
    - December 7, 1941 – U.S. Naval base at Pearl Harbor surprised by Japanese attack, despite U.S. breaking of Japanese codes.
  - April 1943 – Admiral Yamamoto, architect of Pearl Harbor attack, is assassinated by U.S. forces who know his itinerary from decoded messages
  - 1946 – VENONA's first break into Soviet espionage traffic from early 1940s
  - 1948 – Claude Shannon writes a paper that establishes the mathematical basis of information theory

EARLY 20TH CENTURY

- WWI — Zimmerman Telegram
- "Gentlemen do not read each other's mail" — Henry L. Stimson, Secretary of State, 1929
- WWII — golden age of cryptanalysis
  - Japanese Purple (codename **MAGIC**)
  - German Enigma (codename **ULTRA**)

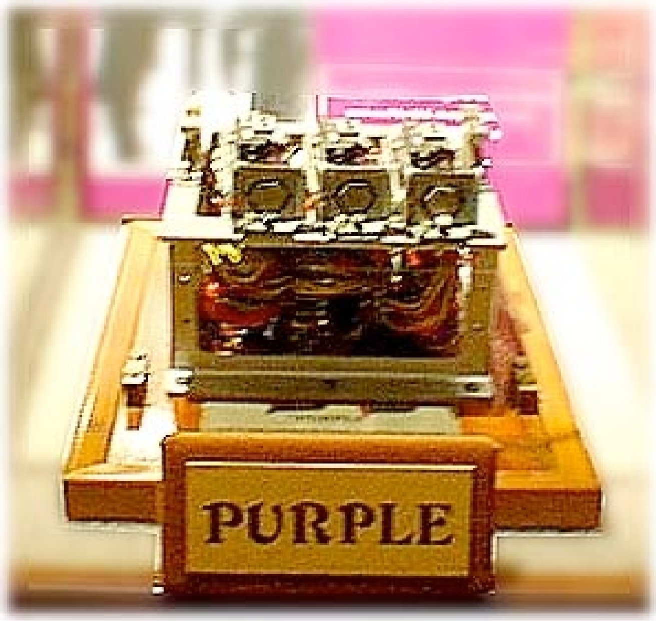
ENIGMA MACHINE

- Encryption machine used by Germans in the WWII, relies on electricity
- Plug board: allowed for pairs of letters to be remapped before the encryption process started and after it ended.
- Light board
- Keyboard
- Set of rotors: user must select three rotors from a set of rotors to be used in the machine. A rotor contains one-to-one mappings of all the letters.
- Reflector (half rotor).



JAPANESE PURPLE MACHINE

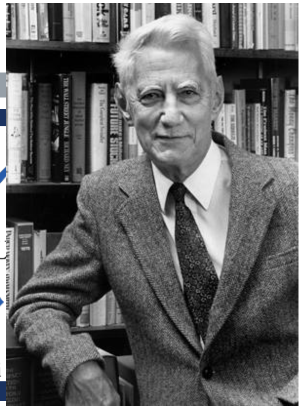
- Electromechanical stepping switch machine modeled after Enigma.
- Used telephone stepping switches instead of rotors
  Pearl Harbor attack
- preparations encoded in Purple, decoded hours before attack.



POST-WWII HISTORY

- Claude Shannon — father of the science of information theory
- Computer revolution — lots of data
- Data Encryption Standard (DES), 70’ s
- Public Key cryptography, 70’ s
- CRYPTO conferences, 80’ s
- Advanced Encryption Standard (AES), 90’ s
- Crypto moved out of classified world

CLAUDE SHANNON



- The founder of Information Theory
- 1949 paper: *Comm. Thy. of Secrecy Systems*
  - http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf
- Confusion and diffusion
  - Confusion— obscure relationship between plaintext and ciphertext
  - Diffusion— spread plaintext statistics through the ciphertext
  - One-time pad only uses confusion, while double transposition only uses diffusion
- Proved that one-time pad is secure

TIMELINE OF CRYPTOGRAPHY

- 1950-1999
  - 1951 - U.S. National Security Agency founded
  - 1964 - David Kahn's *The Codebreakers* is published.
  - August 1964 - Gulf of Tonkin Incident leads U.S. into Vietnam War, possibly due to misinterpretation of signals intelligence by NSA.
  - January 23, 1968 - USS Pueblo, SIGINT ship, is captured by North Korea.

TIMELINE OF CRYPTOGRAPHY

- 1950-1999
  - 1969 - The first hosts of ARPANET, Internet's ancestor, are connected.
  - 1974? - Horst Feistel develops Feistel network block cipher design.
  - 1976 - Data Encryption Standard was published as an official Standard for the United States.
  - 1976 - New Directions in Cryptography published by Diffie and Hellman
  - 1977- RSA public key encryption invented.

TIMELINE OF CRYPTOGRAPHY

- 1950-1999
  - 1981 - Quantum computers proposed .
  - 1989 - the prototype system of World Wide Web at CERN.
  - 1991 - releases the public key encryp prog PGP
  - 1994 - Secure Sockets Layer (SSL) encryption protocol released
  - 1995 - NSA publishes the SHA1 hash algorithm as part of its Digital Signature Standard.

TIMELINE OF CRYPTOGRAPHY

- 2000 and beyond
  - January 14, 2000 – U.S. Government announce restrictions on export of cryptography are relaxed (although not removed).
  - March 2000 – President of the US, Bill Clinton says he doesn't use e-mail to communicate with his daughter, Chelsea Clinton
  - September 6, 2000 – RSA Security Inc. released their RSA algorithm into the public domain, a few days in advance of their U.S. Patent 4,405,829_ expiring.
  - 2001 – Rijndael algorithm selected as the U.S. Advanced Encryption Standard (AES) by National Institute for Standards and Technology (NIST)

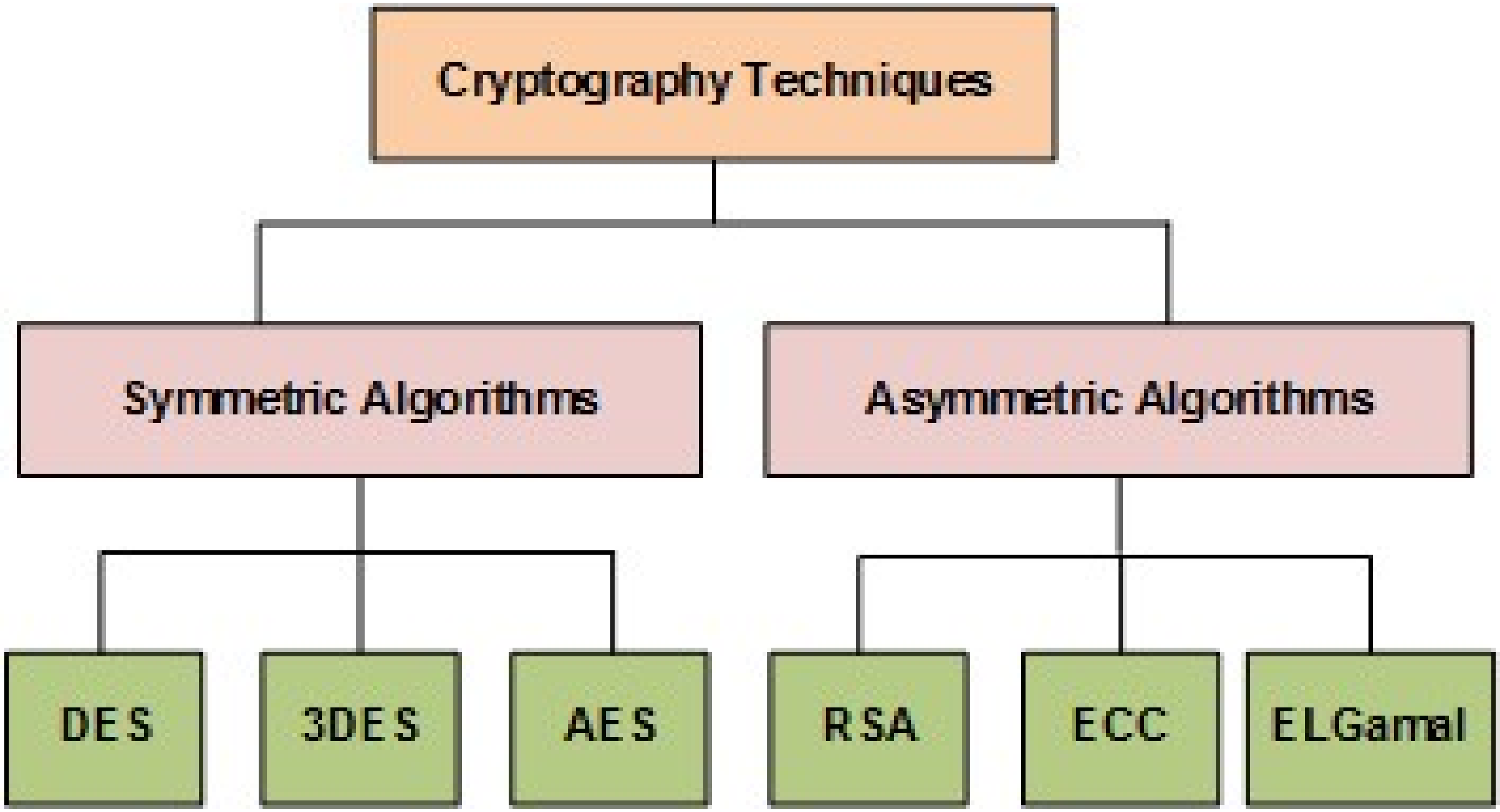
TIMELINE OF CRYPTOGRAPHY

- 2000 and beyond
  - 2004 – the hash MD5 is shown to be vulnerable to practical collision attack
  - 2004 – The first commercial quantum cryptography system becomes available from id Quantique.
  - 2005 – potential for attacks on SHA1 demonstrated
  - 2005 – agents from the U.S. FBI demonstrate their ability to crack WEP using publicly available tools
  - 2015 – year by which NIST suggests that 80-bit keys be phased out.

TAXONOMY

TAXONOMY OF CRYPTOGRAPHY

- Symmetric/Private Key
  - Same key for encryption as for decryption
  - Stream ciphers
  - Block ciphers
- Asymmetric/Public Key
  - Two keys, one for encryption (public), and one for decryption (private)
  - Digital signatures — nothing comparable in symmetric key crypto
- Hash algorithms


Cryptography Techniques
Symmetric Algorithms
Asymmetric Algorithms
DES
3DES
AES
RSA
ECC
ELGamal