Classic Crypto

Overview

- We briefly consider the following classic (pen and paper) ciphers
  - Transposition ciphers
  - Substitution ciphers
  - One-time pad
  - Codebook
- These were all chosen for a reason
  - We see same principles in modern ciphers

Transposition Ciphers

- In transposition ciphers, we transpose (scramble) the plaintext letters
  - The scrambled text is the ciphertext
  - The transposition is the key
- Corresponds to Shannon's principle of **diffusion** (more about this later)
  - This idea is widely used in modern ciphers

Scytale

- Spartans, circa 500 BC
- Wind strip of leather around a rod
- Write message across the rod

T	H	E	T	I	M	E	H	A
S	C	O	M	E	T	H	E	W
A	L	R	U	S	S	A	I	D
T	O	T	A	L	K	O	F	M
A	N	Y	T	H	I	N	G	S

- When unwrapped, letters are scrambled

TSATAHCLONEORTYTMUATIESLHMTS…

Scytale

- Suppose Alice and Bob use Scytale to encrypt a message
  - What is the key?
  - How hard is it for Trudy to break without key?
- Suppose many different rod diameters are available to Alice and Bob…
  - How hard is it for Trudy to break a message?
  - Can Trudy attack messages automatically—without manually examining each **putative** decrypt?

Columnar Transposition

- Put plaintext into rows of matrix then read ciphertext out of columns
- For example, suppose matrix is 3 x 4
  - Plaintext: SEETHELIGHT

$$\begin{bmatrix} S & E & E & T \\ H & E & L & I \\ G & H & T & X \end{bmatrix}$$

  - Ciphertext: SHGEEHELTTIX
- Same effect as Scytale
  - What is the key?

Keyword Columnar Transposition

- For example
  - Plaintext: CRYPTOISFUN
  - Matrix 3 x 4 and keyword MATH

M	A	T	H
C	R	Y	P
T	O	I	S
F	U	N	X

  - Ciphertext: ROUPSXCTFYIN
- What is the key?
- How many keys are there?

Keyword Columnar Transposition

- How can Trudy cryptanalyze this cipher?
- Consider the ciphertext

  VOESA IVENE MRTNL EANGE WTNIM HTMLL ADLTR NISHO DWOEH

- Matrix is n x m for some n and m
- Since 45 letters, $n \cdot m = 45$
- How many cases to try?
- How will Trudy know when she is correct?

Keyword Columnar Transposition

- The ciphertext is

  VOESA IVENE MRTNL EANGE WTNIM HTMLL ADLTR NISHO DWOEH

- If encryption matrix was 9 x 5, then…

0	1	2	3	4
V	E	G	M	I
O	M	E	E	S
E	R	W	E	H
S	T	T	A	O
A	N	N	D	D
I	L	I	L	W
V	E	M	T	O
E	A	H	R	E
N	N	T	N	H

→

2	4	0	1	3
G	I	V	E	M
E	S	O	M	E
W	H	E	R	E
T	O	S	T	A
N	D	A	N	D
I	W	I	L	L
M	O	V	E	T
H	E	E	A	R
T	H	N	N	N

Cryptanalysis: Lesson I

- **Exhaustive key search**
  - Always an option for Trudy
- If keyspace is too large, such an attack will not succeed in a reasonable time
  - Or it will have a low probability of success
- A large keyspace is necessary for security
- But, large keyspace is not sufficient…

Double Transposition

- Plaintext: ATTACK AT DAWN

columns	0	1	2
row 0	A	T	T
row 1	A	C	K
row 2	X	A	T
row 3	X	D	A
row 4	W	N	X

Permute rows and columns

$\Longrightarrow$

columns	0	2	1
row 2	X	T	A
row 4	W	X	N
row 0	A	T	T
row 3	X	A	D
row 1	A	K	C

- Ciphertext: XTAWXNATTXADAKC
- Key?
  - 5 x 3 matrix, perms (2,4,0,3,1) and (0,2,1)

Double Transposition

- How can Trudy attack double transposition?
- Spse Trudy sees 45-letter ciphertext
- Then how many keys?
  - Size of matrix: 3 x 15, 15 x 3, 5 x 9, or 9 x 5
  - A lot of possible permutations!

    $5! \cdot 9! > 2^{25}$ and $3! \cdot 15! > 2^{42}$
- Size of keyspace is greater than 2^{43}
- Is there a shortcut attack?

Double Transposition

- Shortcut attack on double transposition?
- Suppose ciphertext is

ILILWEAHREOMEESANNDDVEGMIERWEHVEMTOSTTAONNTNH

- Suppose Trudy guesses matrix is 9 x 5
- Then Trudy has:
- Now what?
- Try all perms?
  $5! \cdot 9! > 2^{25}$
- Is there a better way?

column	0	1	2	3	4
row 0	I	L	I	L	W
row 1	E	A	H	R	E
row 2	O	M	E	E	S
row 3	A	N	N	D	D
row 4	V	E	G	M	I
row 5	E	R	W	E	H
row 6	V	E	M	T	O
row 7	S	T	T	A	O
row 8	N	N	T	N	H

Double Transposition

- Shortcut attack on double transposition?
- Trudy tries "columns first" strategy

column	0	1	2	3	4
row 0	I	L	I	L	W
row 1	E	A	H	R	E
row 2	O	M	E	E	S
row 3	A	N	N	D	D
row 4	V	E	G	M	I
row 5	E	R	W	E	H
row 6	V	E	M	T	O
row 7	S	T	T	A	O
row 8	N	N	T	N	H

Permute columns ⇒

column	2	4	0	1	3
row 0	I	W	I	L	L
row 1	H	E	E	A	R
row 2	E	S	O	M	E
row 3	N	D	A	N	D
row 4	G	I	V	E	M
row 5	W	H	E	R	E
row 6	M	O	V	E	T
row 7	T	O	S	T	A
row 8	T	H	N	N	N

- Now what?

Cryptanalysis: Lesson II

- **Divide and conquer**
  - Trudy attacks part of the keyspace
  - A great shortcut attack strategy
- Requires careful analysis of algorithm
- We will see this again and again in the attacks discussed later
- Of course, cryptographers try to prevent divide and conquer attacks

Substitution Ciphers

- In substitution ciphers, we replace the plaintext letters with other letters
  - The resulting text is the ciphertext
  - The substitution rule is the key
- Corresponds to Shannon's principle of **confusion** (more on this later)
  - This idea is used in modern ciphers

Ceasar's Cipher

- Plaintext:

  FOURSCOREANDSEVENYEARSAGO

- Key:

Plaintext	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
Ciphertext	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

- More succinctly, key is "shift by 3"

Ceasar's Cipher

- Trudy loves the Ceasar's cipher…
- Suppose ciphertext is
  VSRQJHEREVTXDUHSDQWU

Plaintext	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
Ciphertext	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

- Then plaintext is
  SPONGEBOBSQUAREPANTS

Simple Substitution

- Caesar's cipher is trivial if we adhere to Kerckhoffs' Principle
- We want a substitution cipher with lots of keys
- What to do?
- Generalization of Caesar's cipher…

Simple Substitution

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

Plaintext	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
Ciphertext	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
- That's lots of keys!

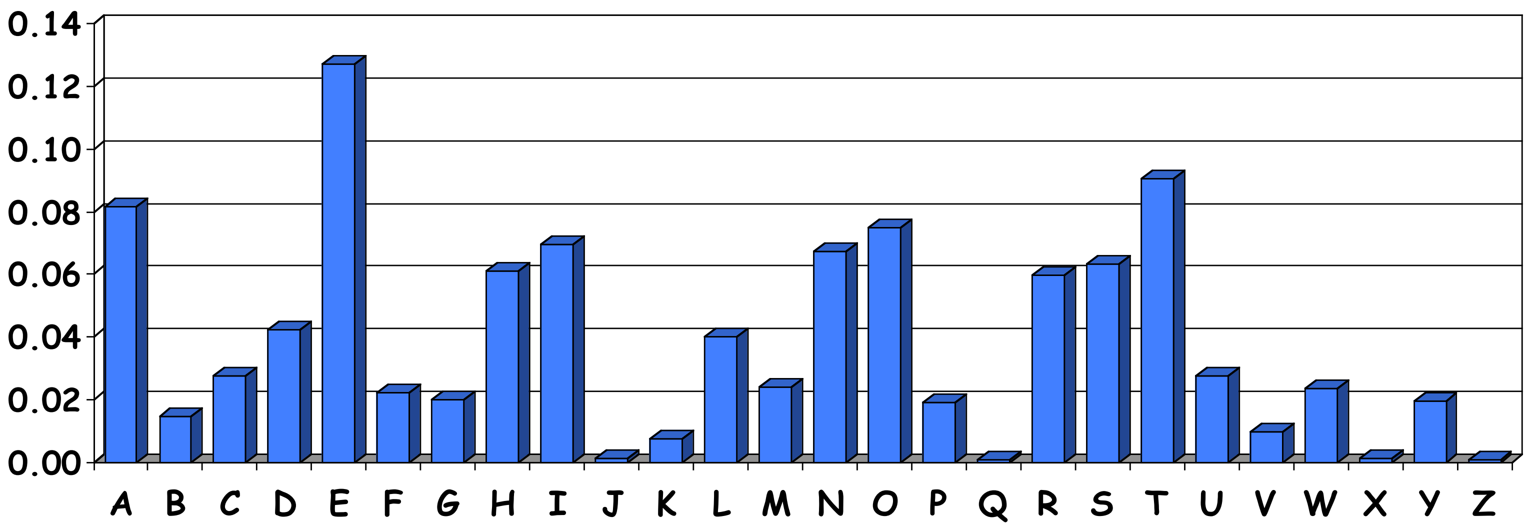
Cryptanalysis of Simple Substitution

- Trudy know a simple substitution is used
- Can she find the key given ciphertext:

PBFPVYFBQXZTYFPBFEQJHDXXQVAPTPQJKTOYQWIPBVW
LXTOXBTFXQWAXBVCXQWAXFQJVWLEQNTOZQGGQLFXQ
WAKVWLXQWAEBIPBFXFQVXGTVJVWLBTPQWAEBFPBFH
CVLXBQUFEVWLXGDPEQVPQGVPPBFTIXPFHXZHVFAGF
OTHFEFBQUFTDHZBQPOTHXTYFTODXQHFTDPTOGHFQP
BQWAQJJTODXQHFOQPWTBDHHIXQVAPBFZQHCFWPFHP
BFIPBQWKFABVYYDZBOTHPBQPQJTQOTOGHFQAPBFEQ
JHDXXQVAVXEBQPEFZBVFOJIWFFACFCCFHQWAUVWFL
QHGFXVAFXQHFUFHILTTAVWAFFAWTEVOITDHFHFQAI
TIXPFHXAFQHEFZQWGFLVWPTOFFA

Cryptanalysis of Simple Substitution

- Trudy cannot try all 2^{88} possible keys
- Can she be more clever?
- Statistics!
- English letter frequency counts:



Cryptanalysis of Simple Substitution

- Ciphertext:

```
PBFPVYFBQXZTYFPBFEQJHDXXQVAPTPQJKTOYQWIPBVWLXTOXBTF
   XQWAXBVCXQWAXFQJVWLEQNTOZQGGQLFXQWAKVWLXQWAEBIPBF
   XFQVXGTVJVWLBTPQWAEBFPBFHCVLXBQUFEVWLXGDPEQVPQGVP
   PBFTIXPFHXZHVFAGFOTHFEFBQUFTDHZBQPOTHXTYFTODXQHFT
   DPTOGHFQPBQWAQJJTODXQHFOQPWTBDHHIXQVAPBFZQHCFWPFH
   PBFIPBQWKFABVYYDZBOTHPBQPQJTQOTOGHFQAPBFEQJHDXXQV
   AVXEBQPEFZBVFOJIWFFACFCCFHQWAUVWFLQHGFXVAFXQHFUFH
   ILTTAVWAFFAWTEVOITDHFHFQAITIXPFHXAFQHEFZQWGFLVWPT
   OFFA
```

- 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

Cryptanalysis: Lesson III

- **Statistical analysis**
  - Statistics might reveal info about key
- Ciphertext should appear random
- But randomness is not easy
  - Difficult to define random (entropy)
- Cryptographers work hard to prevent statistical attacks

Poly-Alphabetic Substitution

- Like a simple substitution, but permutation (“alphabet”) changes
  - Often, a new alphabet for each letter
- Very common in classic ciphers
  - Vigenere cipher is an example
  - Discuss Vigenere later in this section
- Used in WWII-era cipher machines

Affine Cipher

- Number the letters 0 thru 25
  - A is 0, B is 1, C is 2, etc.
- Then affine cipher encryption is defined by $c_i = ap_i + b \pmod{26}$
  - Where p_i is the i^{th} plaintext letter
  - And a and b are constants
  - Require that gcd(a, 26) = 1 (why?)

Affine Cipher

- Encryption: $c_i = ap_i + b \pmod{26}$
- Decryption: $p_i = a^{-1}(c_i - b) \pmod{26}$
- Keyspace size?
  - Keyspace size is $26 \cdot \varphi(26) = 312$
  - Too small to be practical

Vigenere Cipher

- Key is of the form $K = (k_0, k_1, \ldots, k_{n-1})$
  - Where each $k_i \in \{0,1,2,\ldots,25\}$
- Encryption

  $c_i = p_i + k_{i \text{ (mod n)}} \pmod{26}$
- Decryption

  $p_i = c_i - k_{i \text{ (mod n)}} \pmod{26}$
- Nothing tricky here!
- Just a repeating sequence of (shift by n) simple substitutions

Vigenere Cipher

- For example, suppose key is MATH
  - That is, K = (12,0,19,7), since M is letter 12, and so on
- Plaintext: SECRETMESSAGE
- Ciphertext: EEVYQTFLESTNQ
- Encrypt:

S	E	C	R	E	T	M	E	S	S	A	G	E	
18	4	2	17	4	19	12	4	18	18	0	6	4	
+12	0	19	7	12	0	19	7	12	0	19	7	12	
4	4	21	24	16	19	5	11	4	18	19	13	16	(mod 26)
E	E	V	Y	Q	T	F	L	E	S	T	N	Q	

Vigenere Cipher

- Vigenere is just a series of k simple substitution ciphers
- Should be able to do k simple substitution attacks
  - Provided enough ciphertext
- But how to determine k (key length)?
- **Index of coincidence**…

Index of Coincidence

- Assume ciphertext is English letters
- Let n_0 be number of As, n_1 number of Bs, …, n_{25} number of Zs in ciphertext
- Let $n = n_0 + n_1 + \ldots + n_{25}$
- Define index of coincidence

$$I = \frac{\binom{n_0}{2} + \binom{n_1}{2} + \cdots + \binom{n_{25}}{2}}{\binom{n}{2}} = \frac{1}{n(n-1)} \sum_{i=0}^{25} n_i(n_i - 1)$$

- What does this measure?

Index of Coincidence

- Gives the probability that 2 randomly selected letters are the same
- For plain English, prob. 2 letter are same:
  - $p_0^2 + p_1^2 + \ldots + p_{25}^2 \approx 0.065$, where p_i is probability of i^{th} letter
- Then for simple substitution, $I \approx 0.065$
- For random letters, each $p_i = 1/26$
  - Then $p_0^2 + p_1^2 + \ldots + p_{25}^2 \approx 0.03846$
- Then $I \approx 0.03846$ for poly-alphabetic substitution with a very long keyword

Index of Coincidence

- How to use this to estimate length of keyword in Vigenere cipher?
- Suppose keyword is length k, message is length n
  - Ciphertext in matrix with k columns, n/k rows
- Select 2 letters from same columns
  - Like selecting from simple substitution
- Select 2 letters from different columns
  - Like selecting random letters

Index of Coincidence

- Suppose k columns and n/k rows
- Approximate number of matching pairs from same column, but 2 different rows:

$$0.065\binom{\frac{n}{k}}{2}k = 0.065\,\frac{1}{2}\left(\frac{n}{k}\right)\left(\frac{n}{k}-1\right)k = 0.065\left(\frac{n(n-k)}{2k}\right)$$

- Approximate number of matching pairs from 2 different columns, and any two rows:

$$0.03846\binom{k}{2}\left(\frac{n}{k}\right)^2 = 0.03846\,\frac{n^2(k-1)}{2k}$$

Index of Coincidence

- Approximate index of coincidence by:

$$I \approx \frac{0.03846\,\frac{n^2(k-1)}{2k} + 0.065\left(\frac{n(n-k)}{2k}\right)}{\binom{n}{2}}$$

$$= \frac{0.03846n(k-1) + (0.065)(n-k)}{k(n-1)}$$

- Solve for k to find:

$$k \approx \frac{0.02654n}{(0.065 - I) + n(I - 0.03846)}$$

- Use n and I (known from ciphertext) to approximate length of Vigenere keyword

Index of Coincidence: Bottom Line

- A crypto breakthrough when invented
  - By William F. Friedman in 1920s
- Useful against classical and WWII-era ciphers
- Incidence of coincidence is a well-known statistical test
  - Many other statistical tests exists

Hill Cipher

- Hill cipher is not related to small mountains
- Invented by Lester Hill in 1929
  - A pre-modern block cipher
- Idea is to create a substitution cipher with a large "alphabet"
- All else being equal (which it never is) cipher should be stronger than simple substitution

Hill Cipher

- Plaintext, p_0, p_1, p_2, …
- Each p_i is block of n consecutive letters
  - As a column vector
- Let A be n x n invertible matrix, mod 26
- Then ciphertext block c_i is given by
  - $c_i = A\,p_i \pmod{26}$
  - Decryption: $p_i = A^{-1}c_i \pmod{26}$
- The matrix A is the key

Hill Cipher Example

- Let n = 2 and $A = \begin{bmatrix} 22 & 13 \\ 11 & 5 \end{bmatrix}$
- Plaintext

  MEETMEHERE = (12,4,4,19,12,4,7,4,17,4)
- Then

$$p_0 = \begin{bmatrix} 12 \\ 4 \end{bmatrix},\ p_1 = \begin{bmatrix} 4 \\ 19 \end{bmatrix},\ p_2 = \begin{bmatrix} 12 \\ 4 \end{bmatrix},\ p_3 = \begin{bmatrix} 7 \\ 4 \end{bmatrix},\ p_4 = \begin{bmatrix} 17 \\ 4 \end{bmatrix}$$

- And

$$c_0 = \begin{bmatrix} 4 \\ 22 \end{bmatrix},\ c_1 = \begin{bmatrix} 23 \\ 9 \end{bmatrix},\ c_2 = \begin{bmatrix} 4 \\ 22 \end{bmatrix},\ c_3 = \begin{bmatrix} 24 \\ 19 \end{bmatrix},\ c_4 = \begin{bmatrix} 10 \\ 25 \end{bmatrix}$$

- Ciphertext:

  (4,22,23,9,4,22,24,19,10,25) = EWXJEWYTKZ

Hill Cipher Cryptanalysis

- Trudy suspects Alice and Bob are using Hill cipher, with n x n matrix A
- Suppose Trudy knows n plaintext blocks
  - Plaintext blocks $p_0,p_1,\ldots,p_{n-1}$
  - Ciphertext blocks $c_0,c_1,\ldots,c_{n-1}$
- Let P be matrix with columns $p_0,p_1,\ldots,p_{n-1}$
- Let C be matrix with columns $c_0,c_1,\ldots,c_{n-1}$
- Then $AP = C$ and $A = CP^{-1}$ if P^{-1} exists

Cryptanalysis: Lesson IV

- **Linear** ciphers are weak
  - Since linear equations are easy to solve
- Strong cipher must have nonlinearity
  - Linear components are useful
  - But cipher cannot be entirely linear
- Cryptanalyst try to approximate nonlinear parts with linear equations

One-time Pad

- A provably secure cipher
- No other cipher we discuss is provably secure
- Why not use one-time pad for everything?
  - Impractical for most applications
  - But it does have its uses

One-time Pad Encryption

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

Encryption: Plaintext ⊕ Key = Ciphertext

	h	e	i	l	h	i	t	l	e	r
Plaintext:	001	000	010	100	001	010	111	100	000	101
Key:	111	101	110	101	111	100	000	101	110	000
Ciphertext:	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

	s	r	l	h	s	s	t	h	s	r
Ciphertext:	110	101	100	001	110	110	111	001	110	101
Key:	111	101	110	101	111	100	000	101	110	000
Plaintext:	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**":

	s	r	l	h	s	s	t	h	s	r
Ciphertext:	110	101	100	001	110	110	111	001	110	101
"**key**":	101	111	000	101	111	100	000	101	110	000
"Plaintext":	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:

	s	r	l	h	s	s	t	h	s	r
Ciphertext:	110	101	100	001	110	110	111	001	110	101
"Key":	111	101	000	011	101	110	001	011	101	101
"Plaintext":	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 the same way as the pad?

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 Cipher

- Literally, a book filled with "codes"
  - More precisely, 2 codebooks, 1 for encryption and 1 for decryption
- Key is the codebook itself
- Security of cipher requires physical security for codebook
- Codebooks widely used thru WWII

Codebook Cipher

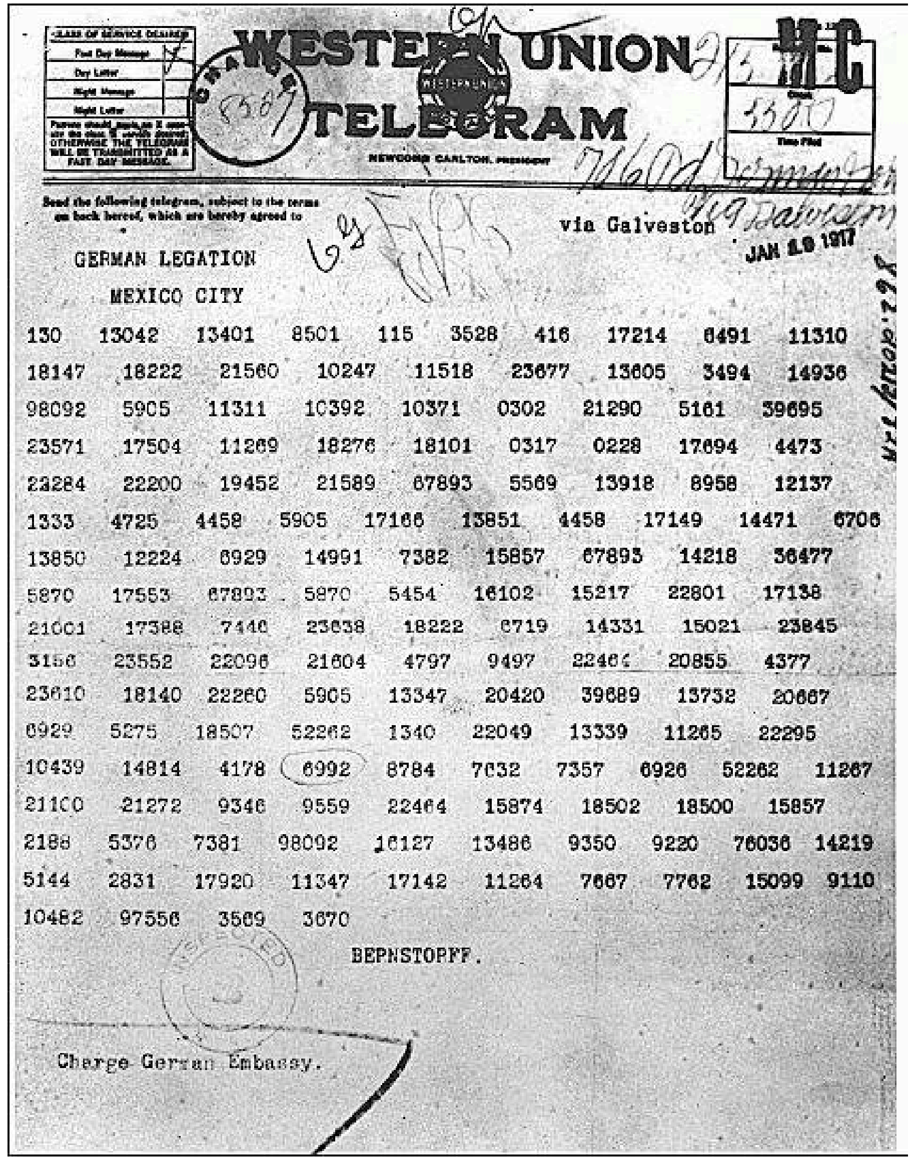
- Literally, a book filled with "codewords"
- Zimmerman Telegram encrypted via codebook

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…



WESTERN UNION TELEGRAM

via Galveston

GERMAN LEGATION

MEXICO CITY

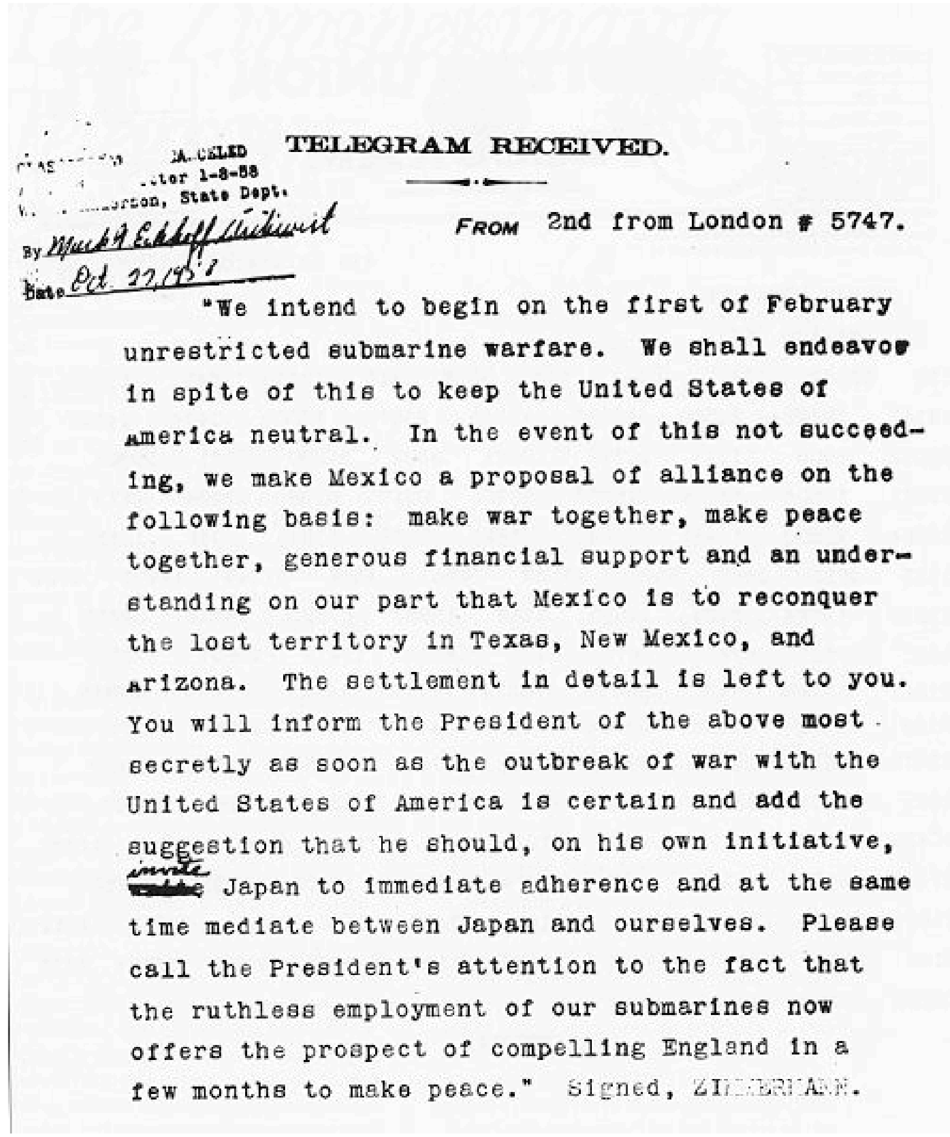
130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 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

BEPNSTOPFF.

Charge German Embassy.

Zimmerman Telegram Decrypted

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



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.

Codebook Cipher

- Codebooks are susceptible to statistical analysis
  - Like simple substitution cipher, but lots of data required to attack a codebook
- Historically, codebooks very popular
- To extend useful life of a codebook, an **additive** was usually used

Codebook Additive

- Codebook **additive** is another book filled with "random" number
- Sequence of additive numbers added to codeword to yield ciphertext

Codebook Additive

- Usually, starting position in additive book selected at random by sender
- Starting additive position usually sent "in the clear" with the ciphertext
  - Part of the message indicator (**MI**)
  - Modern term: initialization vector (**IV**)
- Why does this extend the useful life of a codebook?

Cryptanalysis: Summary

- Exhaustive key search
- Divide and conquer
- Statistical analysis
- Exploit linearity
- Or any combination thereof (or anything else you can think of)
- All's fair in love and war…
  - …and cryptanalysis!