Computer Security

# Classical Encryption Techniques

There are two types of encryption: one that will prevent your sister from reading your diary and one that will prevent your government.

-Bruce Schneier

Tamer ABUHMED
Department of Computer Science & Engineering
Sungkyunkwan University

SUNG KYUN KWAN UNIVERSITY

# Outline

- Crypto terminologies
- Symmetric key crypto Scenario
- Basic types of Symmetric Encryption (Substitution, Permutation, Transposition)
- One-Time Pad
- Codebook Cipher
- More Crypto terminologies

# Crypto (Cryptography )

- **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)

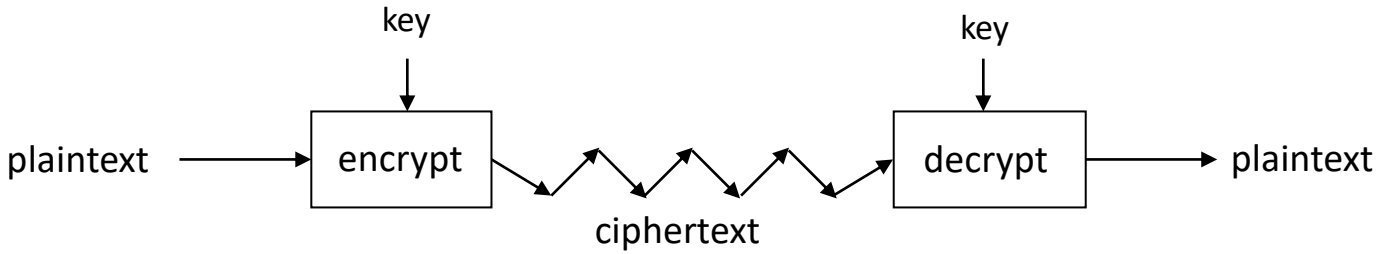
# How to Speak Crypto

- 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

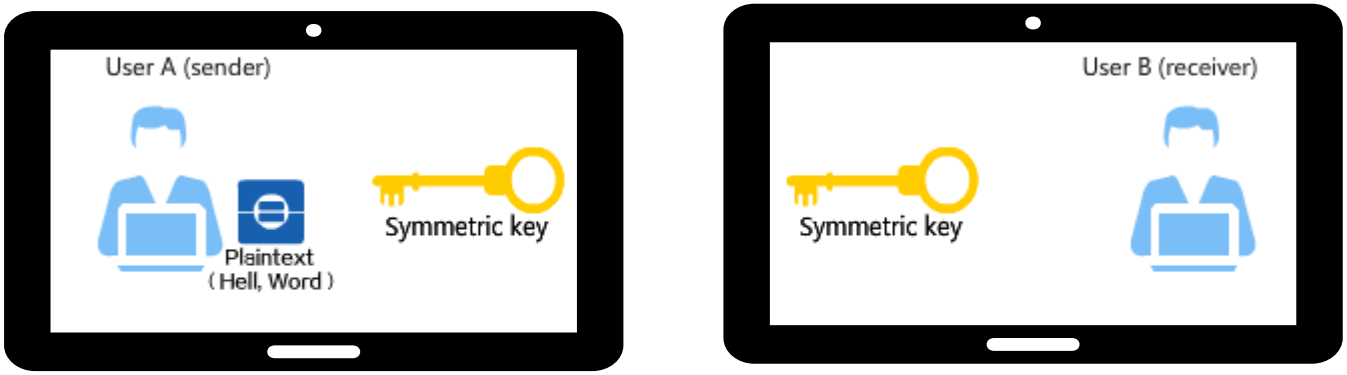
# Crypto

- Basic assumptions
  - The system is completely known to the attacker
  - Only the key is secret
  - That is, crypto algorithms are not secret
- This is known as **Kerckhoffs' Principle**
- 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 view of symmetric key crypto



# Simple Substitution

- 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:
  IRXUVFRUHDQGVHYHQBHDUVDJR
- Shift by 3 is “Caesar’s cipher”

# Ceasar's Cipher Decryption

- Plaintext: spongebobsquarepants
  - Suppose we know a Ceasar's cipher is being used:

| 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 |

  - Given ciphertext:
    VSRQJHEREVTXDUHSDQWV

[Ceasar's Cipher practice]

# Not-so-Simple Substitution

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

| 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 | 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 |

# Cryptanalysis I: Try Them All

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

# Least-Simple Simple Substitution

- In general, simple substitution key can be any **permutation** of letters
  - Not necessarily a shift of the alphabet
- 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!

[Cipher Wheel Practice]

# How large of a keyspace is large enough?

- Suppose Trudy has a fast computer (or group of computers) that's able to test $2^{40}$ keys each second.
- That means, a keyspace of size $2^{56}$ can be exhausted in $2^{16}$ seconds (18 hours).
- A keyspace of size $2^{64}$ would take more than half a year.
- A keyspace of size $2^{128}$ would require more than nine quintillion* years.
- A keyspace of size $2^{88}$ would require more than 8900 millennia**

* Quintillion = $10^{18}$

** Millennia = 1000

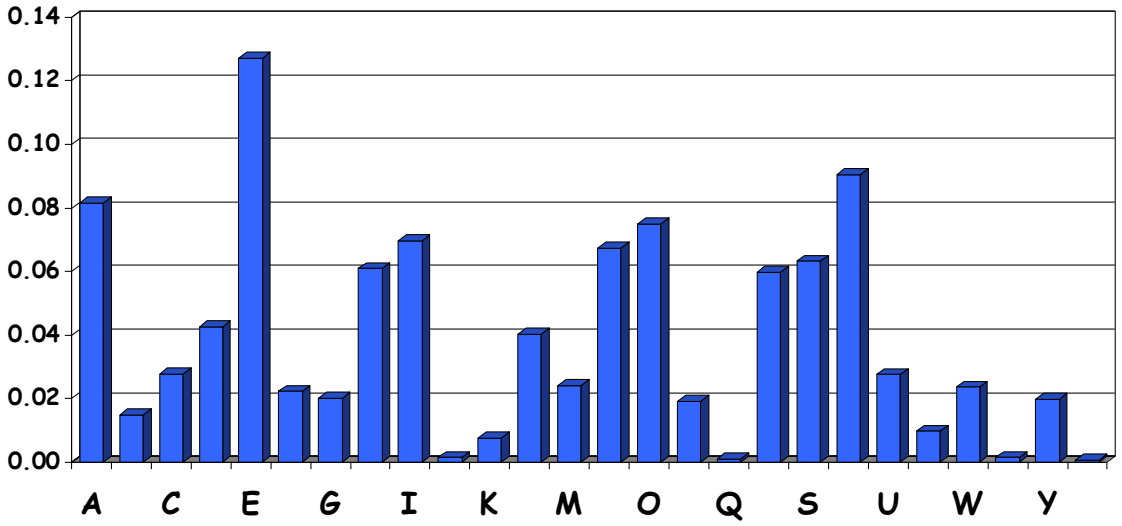
# Cryptanalysis II: Be Clever

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

OAKQH EO PDA YWLEPWH KB OKQPD GKNAW SEPD W IQJEYELWH LKLQHWPEKJ KB KRAN PAJ IEHHEKJ WJZ W IAPNKLKHEPWJ LKLQHWPEKJ PKPWHEJC KRAN PSAJPU IEHHEKJ OAKQH EO XU BWN OKQPD GKNAW HWNCAOP YEPU WJZ KJA KB AWOP WOEWO BEJWJYEWH WJZ YQHPQNWH YAJPANO W BWOYEJWPEJC XHAJZ KB WJYEAJP PNWZEPEKJO WJZ YQPPEJC AZCA ZECEPWH PAYDJKHKCU DKIA PK AJZHAOO OPNAAP BKKZ RAJZKNO WJZ RWOP JECDPHEBA ZEOPNEYPO WJ ATPNWKNZEJWNEHU DECD LNAOOQNA AZQYWPEKJWH OUOPAI WJZ OANAJA XQZZDEOP PAILHAO W ZUJWIEY PNAJZ OAPPEJC UKQPD YQHPQNA WJZ KBPAJ YNQODEJC YKJBKNIEOI ATPNWKNZEJWNU WNYDEPAYPQNA WJZ AJZHAOO IKJKPKJKQO NKSO KB CNAU WLWNPIAJP XQEHZEJCO OAKQH EO W YEPU BEHHAZ SEPD OPWNG YKJPNWOPO YKJPNWZEYPEKJO WJZ LWNWZKTAO

# Cryptanalysis II

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



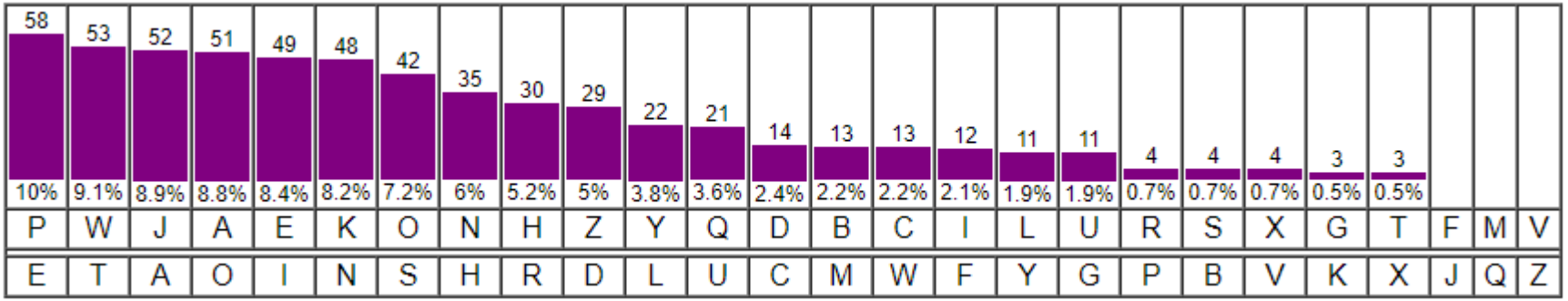
# Cryptanalysis II

- Ciphertext:

OAKQH EO PDA YWLEPWH KB OKQPD GKNAW SEPD W IQJEYELWH LKLQHWPEKJ KB KRAN PAJ IEHHEKJ WJZ W IAPNKLKHEPWJ LKLQHWPEKJ PKPWHEJC KRAN PSAJPU IEHHEKJ OAKQH EO XU BWN OKQPD GKNAW HWNCAOP YEPU WJZ KJA KB AWOP WOEWO BEJWJYEWH WJZ YQHPQNWH YAJPANO W BWOYEJWPEJC XHAJZ KB WJYEAJP PNWZEPEKJO WJZ YQPPEJC AZCA ZECEPWH PAYDJKHKCU DKIA PK AJZHAOO OPNAAP BKKZ RAJZKNO WJZ RWOP JECDPHEBA ZEOPNEYPO WJ ATPNWKNZEJWNEHU DECD LNAOOQNA AZQYWPEKJWH OUOPAI WJZ OANAJA XQZZDEOP PAILHAO W ZUJWIEY PNAJZ OAPPEJC UKQPD YQHPQNA WJZ KBPAJ YNQODEJC YKJBKNIEOI ATPNWKNZEJWNU WNYDEPAYPQNA WJZ AJZHAOO IKJKPKJKQO NKSO KB CNAU WLWNPIAJP XQEHZEJCO OAKQH EO W YEPU BEHHAZ SEPD OPWNG YKJPNWOPO YKJPNWZEYPEKJO WJZ LWNWZKTAO

- Analyze this message using statistics below

Ciphertext frequency counts:



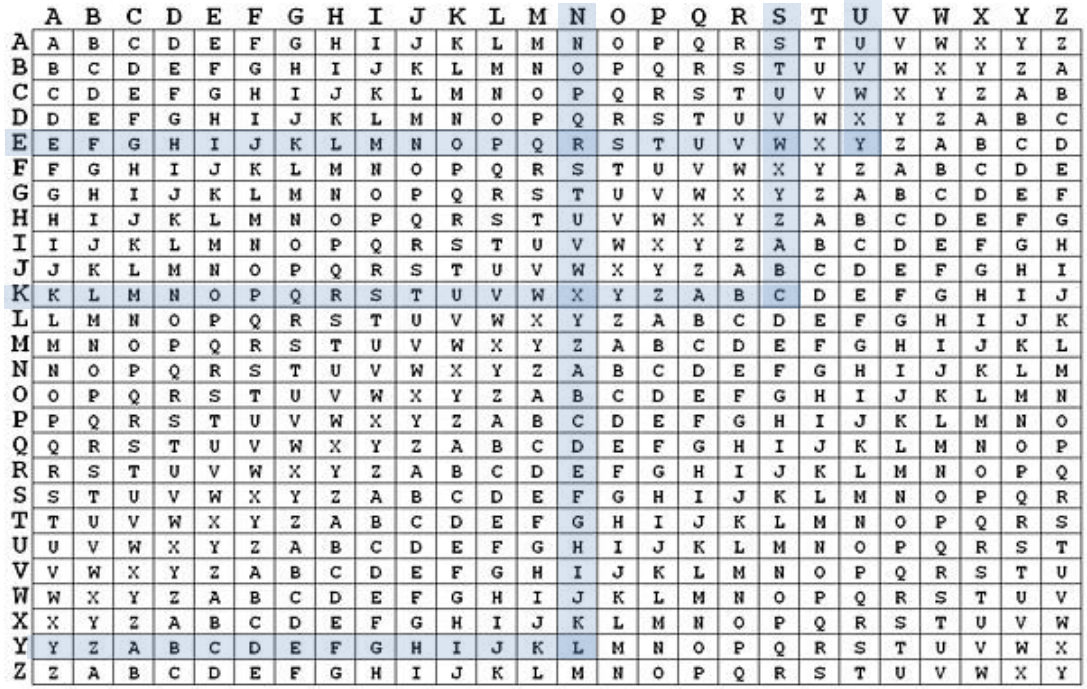

[Cryptanalysis practice]

# Vigenère Substitution

SUNGKYUNKWAN UNIVERSITY

KEY KEY KEY KEY KEY KEY KEY

CYLQOWERIGEL ERGFIPCMRI



| | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | 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 |
| B | 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 | A |
| C | C | 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 |
| D | 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 |
| E | 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 | D |
| F | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| G | G | 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 |
| H | 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 |
| I | 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 | H |
| J | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| K | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| L | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| M | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| N | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| O | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| P | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| Q | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| R | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| S | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| T | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| U | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| V | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
| W | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| X | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| Y | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| Z | Z | 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 |

[Vigenère encryption practice]

# Vigenère cipher cryptoanalysis

WOSSP SW RLO GYTSXYP YJ QSEXF OYVCE GMRL K QSRSGGTKP
NSZYJEDMMR YJ MZOV RIX QGPVMMR KRB E WIRVYTMPSXYR
ZSNYVERMYR RSDEJMXK MZOV RAORRC WMJPSSL WOSSP SW ZC PEP
WYYRL USPIK PYVQIQX MMRC KRB SXI MJ OEQX KWGEC JGRKRAMKP
YRN GSPDYPEV GCRDIPW K JYWMMLEDMLK LPCRN SD EXGGIXX
RVKHGXSSLW KRB GEXRMXK CHQI BMQMREV XCGRRMPYKW LYQC XY
ILHVIQW CXPIOX DSYH TIXHMVC ELH FEQX XMELDPGJO HGWDVGGDW
YR OBRVKSPHSRYVSPW LSKF TBIQWEVC INYAEDMMRKP QCCXCQ KRB
WOVCRO FSHNLGWD XCQZPCW K HWRKQGG DVCRN WCXDMLK ISSXR
GSPDYPI KRB SPXCR MVSWRMLK MSLJYVKMCQ CBDVYSBHGRKVW
EBGFMDIAXEVC EXH CRNPCWC QMRYXMRYYQ VYAQ SP KPII
ENEBXKIXX ZYSPBMXKQ WOSSP SW Y GSXW JSPJIN AGXR WREBO
ASXXPECXQ GYRRVKHGGDMMRC ELH ZEPENSVIC AGXR STIB XCR
WMJPSSL TOSNPO E DMQYPI DLYX NSSFVIQ MP CMY SRAPEHC
ROMELLSPMXK AMDMCW KRB WEFSVLW QIYYJ MC XFI VEPKOWR GSXW
MX WMYDL ISBIY EXH SRAYCWDMMRKFJC DLC IMSLSWMA TYPGXSGYP
KRB GEPRYBEJ LEF MJ DLC RKXGSX FW WYQC QOEQYBIQ MD MQ XRI
QIMSLH VEPKOWR YBFYR KKEPYQCVKXGSX SL XRI NPKRCX KJRIB
KPIKXCV

# Cryptanalysis: Terminology

- Cryptosystem is **secure** if best know attack is to try all keys
  - Exhaustive key search, that is
- Cryptosystem is **insecure** if ***any*** shortcut attack is known
- But then insecure cipher might be harder to break than a secure cipher!
  - What the … ?

# Double Transposition

- Plaintext: attackxatxdawn,

  Encryption Operations: permute rows $(1, 2, 3) \rightarrow (3, 2, 1)$

  Then transpose the columns $(1, 2, 3, 4) \rightarrow (4, 2, 1, 3)$

$$\begin{bmatrix} a & t & t & a \\ c & k & a & t \\ d & a & w & n \end{bmatrix} \longrightarrow \begin{bmatrix} d & a & w & n \\ c & k & a & t \\ a & t & t & a \end{bmatrix} \longrightarrow \begin{bmatrix} n & a & d & w \\ t & k & c & a \\ a & t & a & t \end{bmatrix}$$

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

$$\begin{bmatrix} N & A & D & W \\ T & K & C & A \\ A & T & A & T \end{bmatrix} \longrightarrow \begin{bmatrix} D & A & W & N \\ C & K & A & T \\ A & T & T & A \end{bmatrix} \longrightarrow \begin{bmatrix} A & T & T & A \\ C & K & A & T \\ D & A & W & N \end{bmatrix}$$

# One-Time Pad Encryption (Vernam cipher)

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 following "**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

Or 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

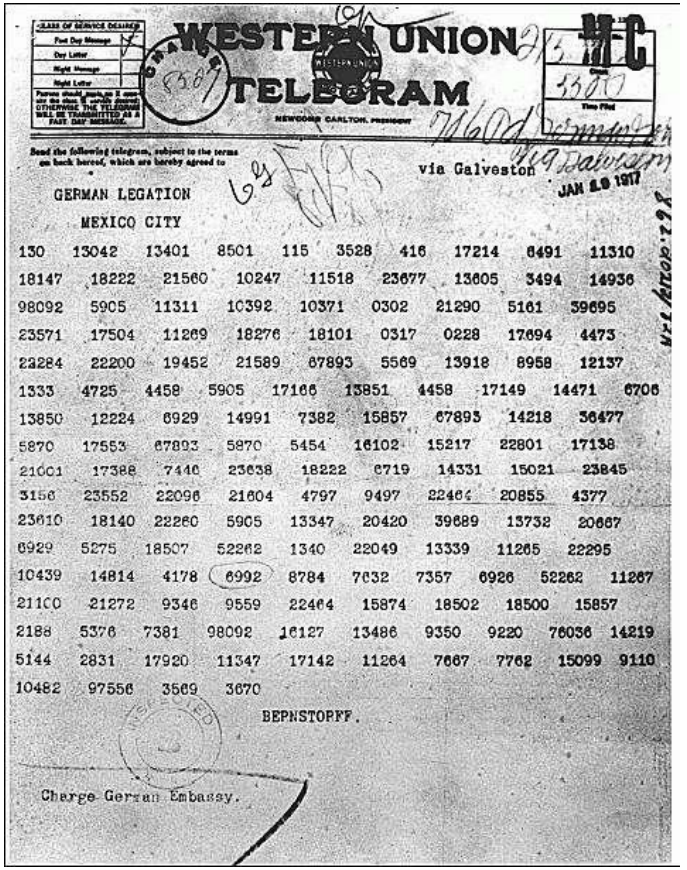
- **Provably** secure…
  - Ciphertext provides **no** info about plaintext
  - All plaintexts are equally likely
- …but, only when be used correctly
  - Pad must be random, used only once
  - Pad is known only to sender and receiver
- Note: pad (key) is same size as message
- So, why not distribute msg instead of pad?

# 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 about this later…



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
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.

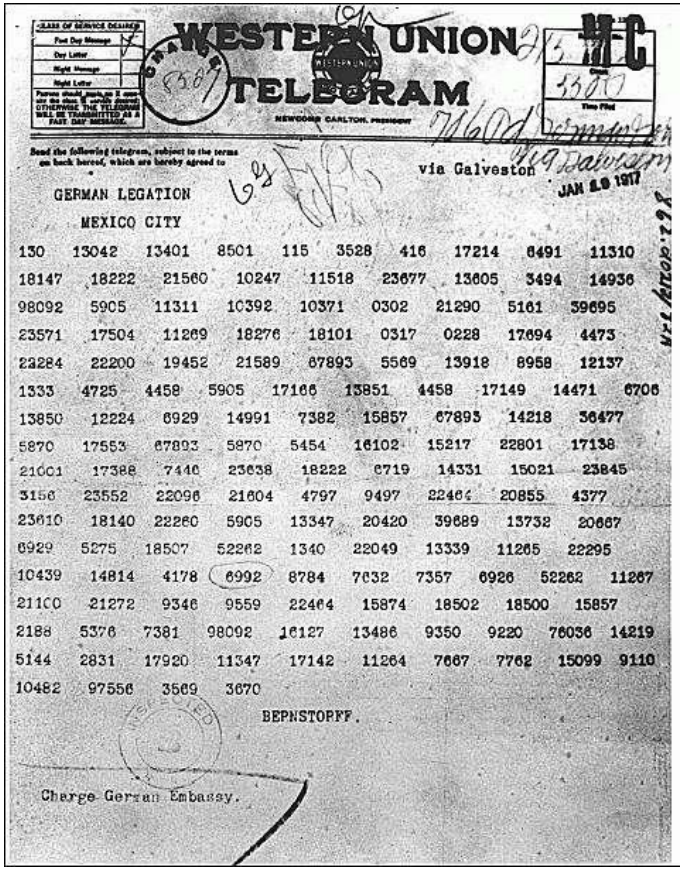
Charge German Embassy.

# Codebook Cipher: Additive

- Codebooks also (usually) use **additive**
- Additive — book of "random" numbers
  - Encrypt message with codebook
  - Then choose position in additive book
  - Add additives to get ciphertext
  - Send ciphertext and additive position (MI)
  - Recipient subtracts additives before decrypting
- Why use an additive sequence?

# Zimmerman Telegram

- Perhaps most famous codebook ciphertext ever
- A major factor in U.S. entry into World War I



WESTERN UNION TELEGRAM

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
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

BEPNSTORFF.

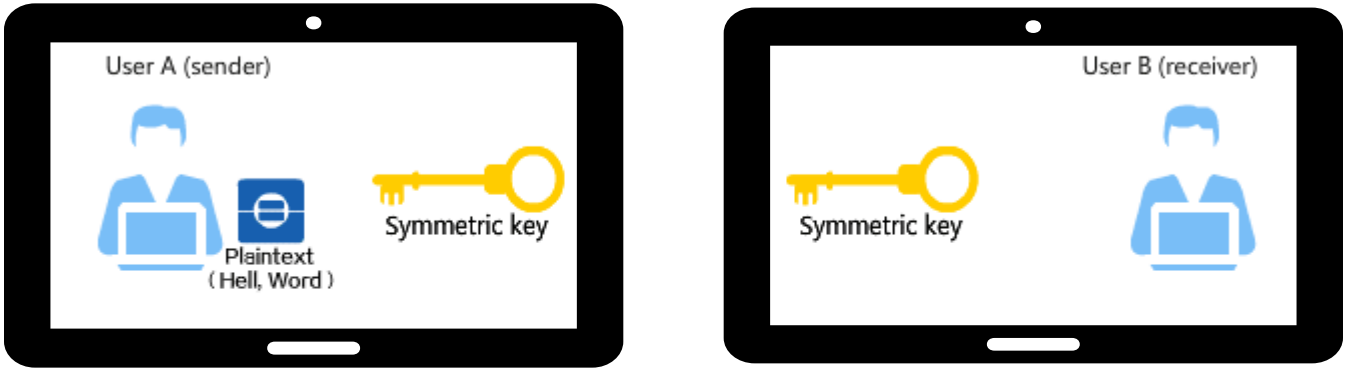
Charge German Embassy.

# Claude Shannon

- The founder of Information Theory
- 1949 paper: *Comm. Thy. of Secrecy Systems*
- Fundamental concepts
  - **Confusion** — obscure relationship between plaintext and ciphertext
  - **Diffusion** — spread plaintext statistics through the ciphertext
- Proved one-time pad is secure
- One-time pad is confusion-only, while double transposition is diffusion-only

# Taxonomy of Cryptography

- **Symmetric Key**
  - **Same key** for encryption and decryption
  - Two types: Stream ciphers, Block ciphers



# Taxonomy of Cryptography

- **Public Key** (or asymmetric cryptography)
  - Two keys, one for encryption (public), and one for decryption (private)
  - And digital signatures — nothing comparable in symmetric key crypto

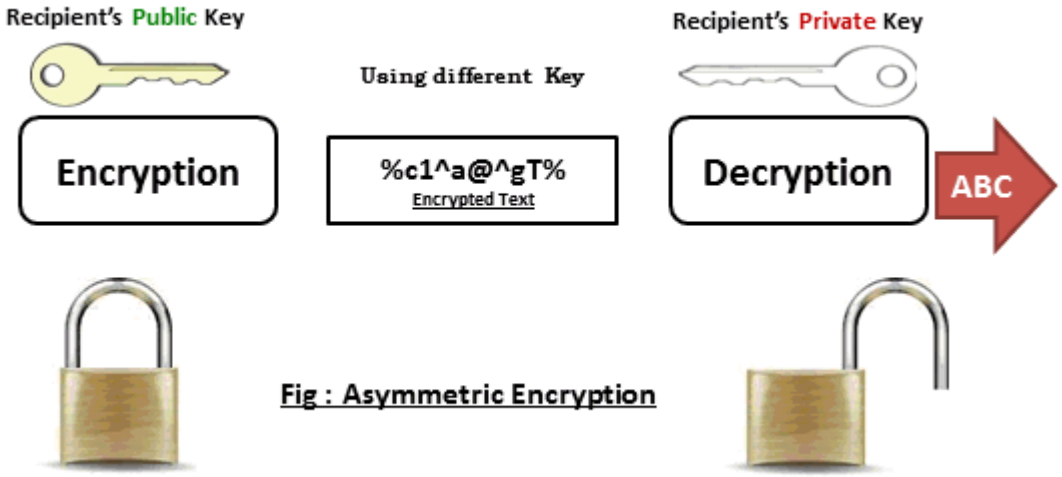



Fig : Asymmetric Encryption

# Taxonomy of Cryptography

- **Hash algorithms**
  - Can be viewed as “one way” crypto


Fig : Encryption and Decryption


Fig : Hashing Concept

# Summary

- Crypto terminologies
- Symmetric key crypto Scenario
- Basic types of Symmetric Encryption (Substitution, Permutation, Transposition)
- One-Time Pad
- Codebook Cipher
- More Crypto terminologies