Basics of Cryptography

What we have learned

- Principles of computer security
  - Confidentiality
  - Integrity
  - Availability
  - Authenticity
  - Accountability
  - Non-repudiation
- Trust is inevitable somewhere
- Human factor also key in computer security
- Broader issues related to computer security, such as ethics, law, and privacy

Check all answers that apply

I have a file in a UNIX file system with **READ-ONLY** access right. If someone steals my credential to log into the file system, what security principles can be violated?

- A: Confidentiality
- B: Availability
- C: Integrity
- D: Authenticity

Check all answers that apply

I have a file in a UNIX file system with **READ-ONLY** access right. If someone steals my credential to log into the file system, what security principles can be violated?

- **A: Confidentiality**
- B: Availability
- C: Integrity
- **D: Authenticity**

Crypto Basics

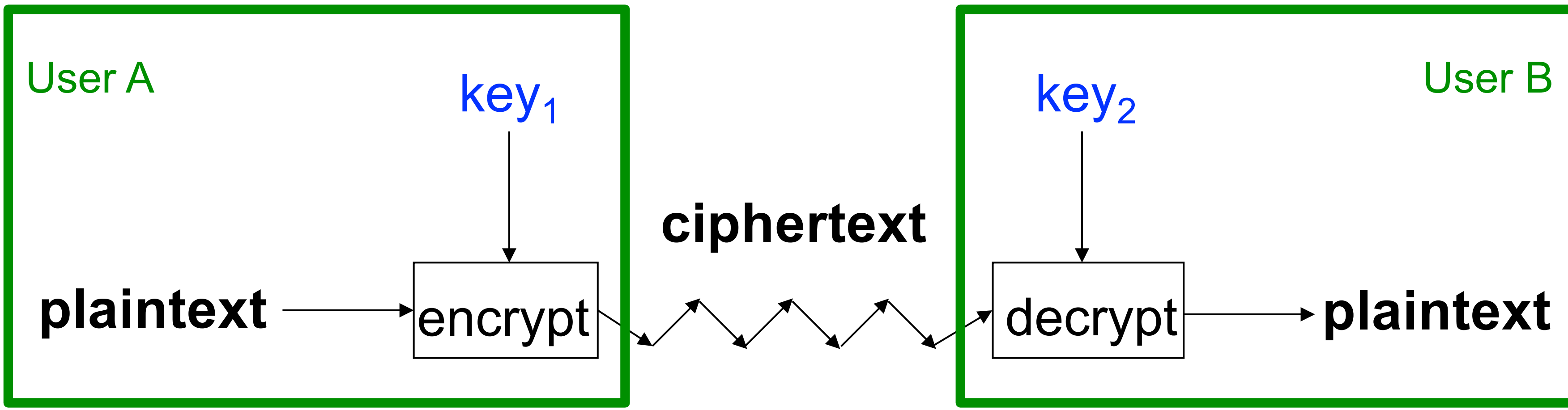
Crypto Terms

- **Crypto – from Greek “krypto” = hide**
- Recently, crypto means Cryptocurrency
- **Cryptography** — making “secret codes”
- **Cryptanalysis** — breaking “secret codes”

Crypto Terms

- A **cipher** is used to **encrypt** the **plaintext**
  - The *algorithm* to encrypt plaintext
- The result of encryption is **ciphertext**
- We **decrypt** ciphertext to recover plaintext
- A **key** is used to configure a cryptosystem
  - The *configuration* of the algorithm
- A **symmetric key** cryptosystem uses the same key to encrypt as to decrypt
- An **asymmetric key** cryptosystem uses different keys for encryption and decryption

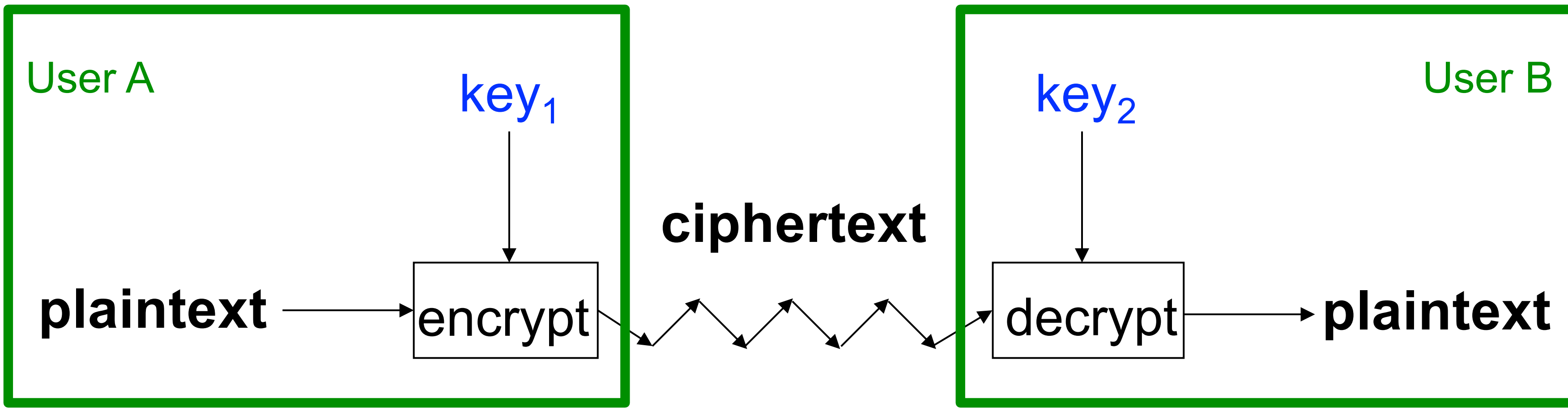
Illustration of a cryptosystem



$Key_1 = Key_2$: Symmetric

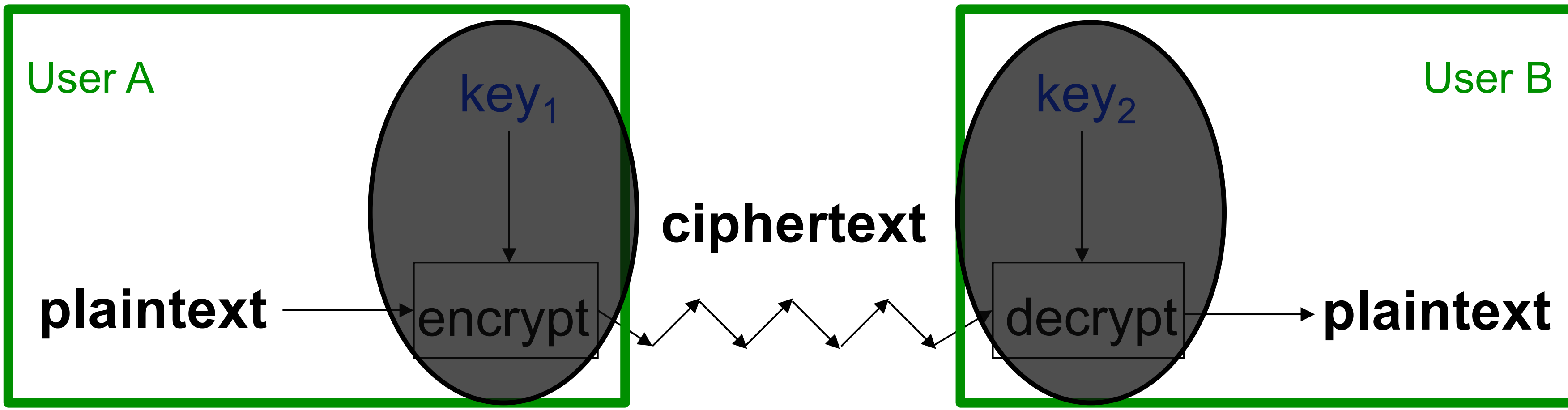
$Key_1 \neq Key_2$: Asymmetric

Illustration of a cryptosystem

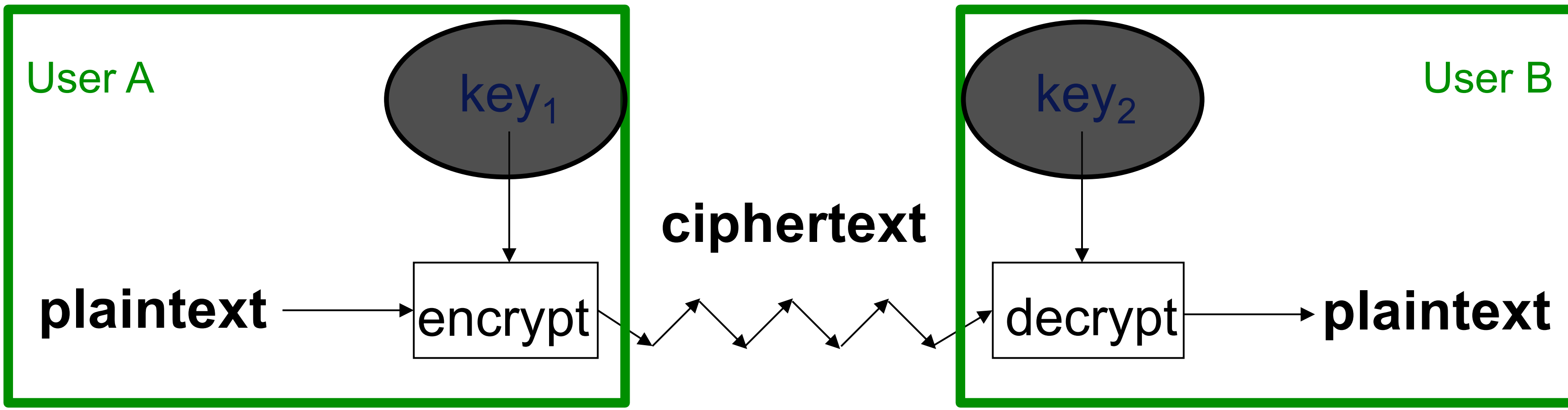


How to protect the security of this cryptosystem?

Case 1: both key and cipher are secret



Case 2: key is secret



Kerckhoffs' Principle

- **Kerckhoff's principle:** the cipher method must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.
- Kerckhoff's principle demands that <u>security must rely solely on the secrecy of the keys</u>.
- In other words,
  - Algorithm must **not** be required to be secret
  - Configuration must be secret

Why Kerckhoffs' Principle?

- Easier to maintain key than algorithm
  - Key is short, algorithm is long
- Easier to replace key than algorithm
  - In case that the key is exposed, it is much easier to replace the key than to replace the algorithm (and the software that implements it)
- Easier to use different key with same algorithm
  - In case many pairs of people need to encrypt their communications, it's much easier for all parties to use the same algorithm/program but different keys, than for everyone to use a different algorithm/program
- Algorithm can be reverse engineered
- Algorithm can be improved under many eyeballs

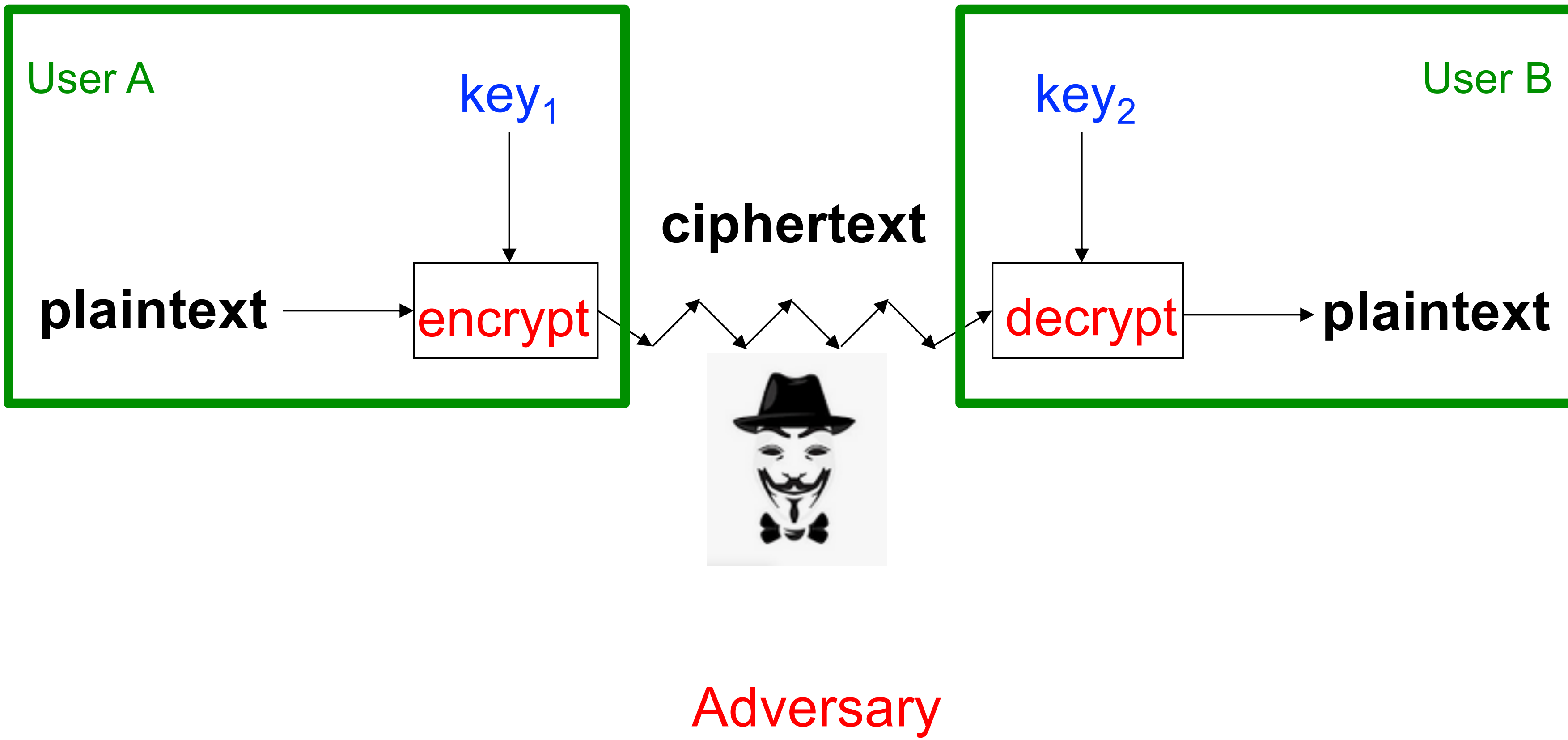
Is Kerckhoffs' Principle enough?

- Is it secure to rely solely on keeping the keys secret when the algorithm is exposed to everyone?
- A fast machine can verify 2^{40} keys per second
  - A keyspace of size 2^{56}
    - Keyspace: the total number of possible keys
    - 2^{16} seconds = 18 hours for exhaustive key search
  - A keyspace of size 2^{128} (128 bits)
    - More than 9 quintillion($9 \ast 10^{18}$) years
    - **Impractical** for exhaustive key search

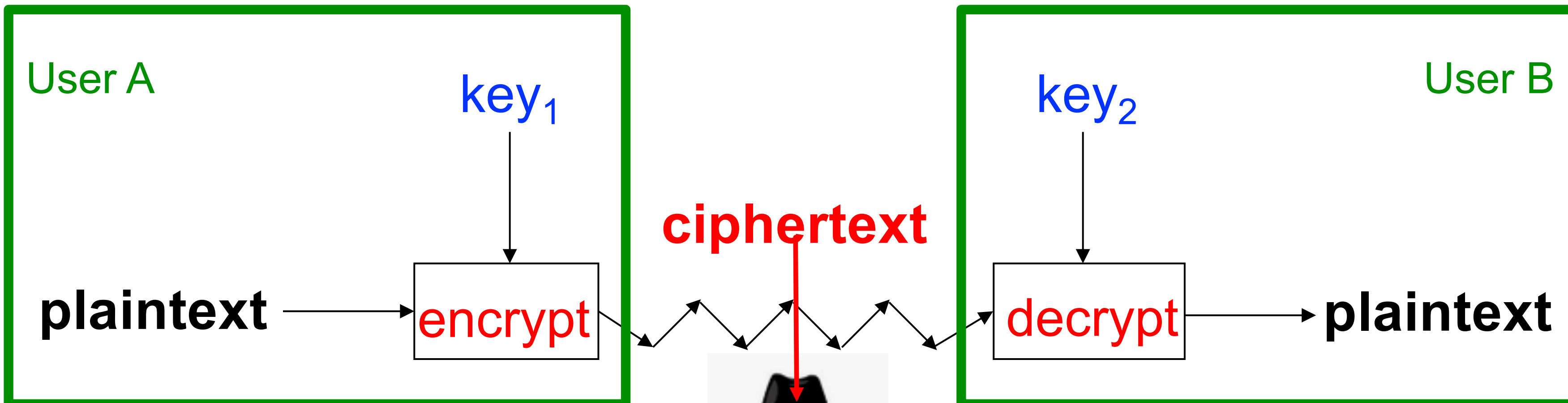
Cryptanalysis: Terminology

- A cryptosystem is **secure** if best known attack is to try all keys
- A cryptosystem is **insecure** if ***any*** shortcut attack is known
- **Secure Cipher**: mathematically proved secure
  - Very few, not practical
- Which is more difficult to break?
  - A secure cipher with a small number of keys
  - An insecure cipher with a large number of keys
- Insecure cipher might be harder to break than a secure cipher!

Attack scenarios against a cipher by adversary



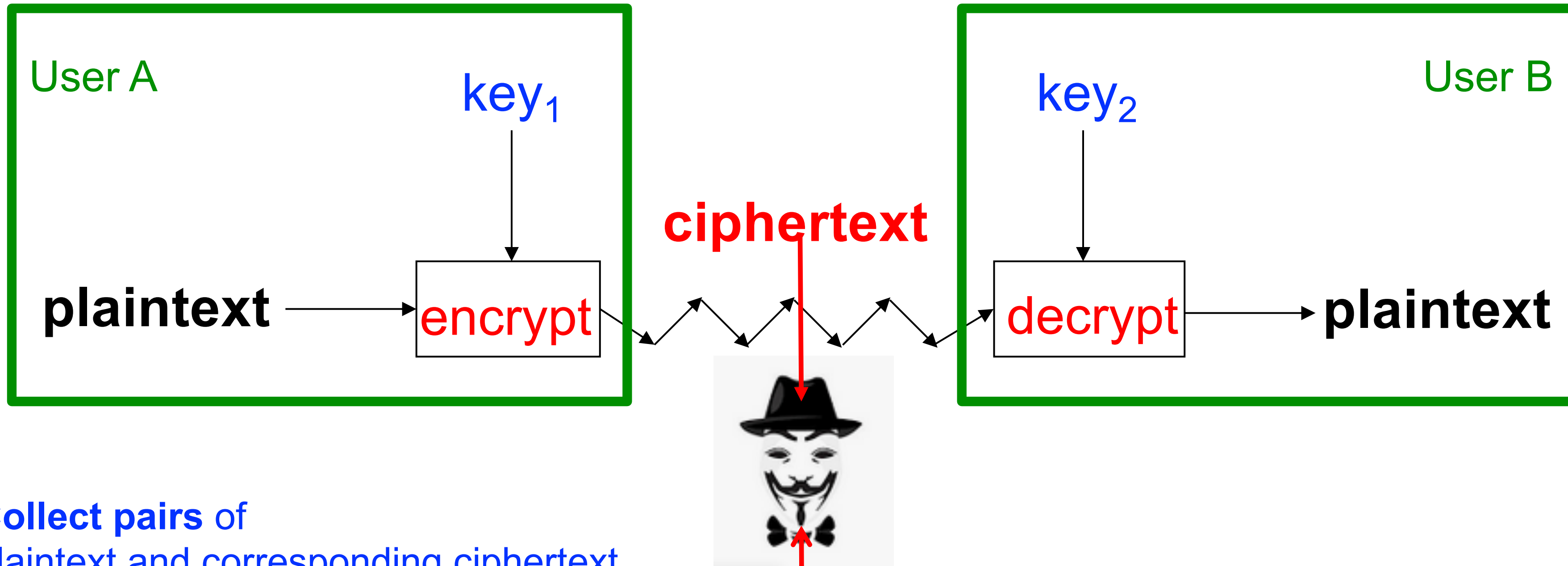
1. Ciphertext Only Attack



Most difficult type of attack to succeed with

Adversary

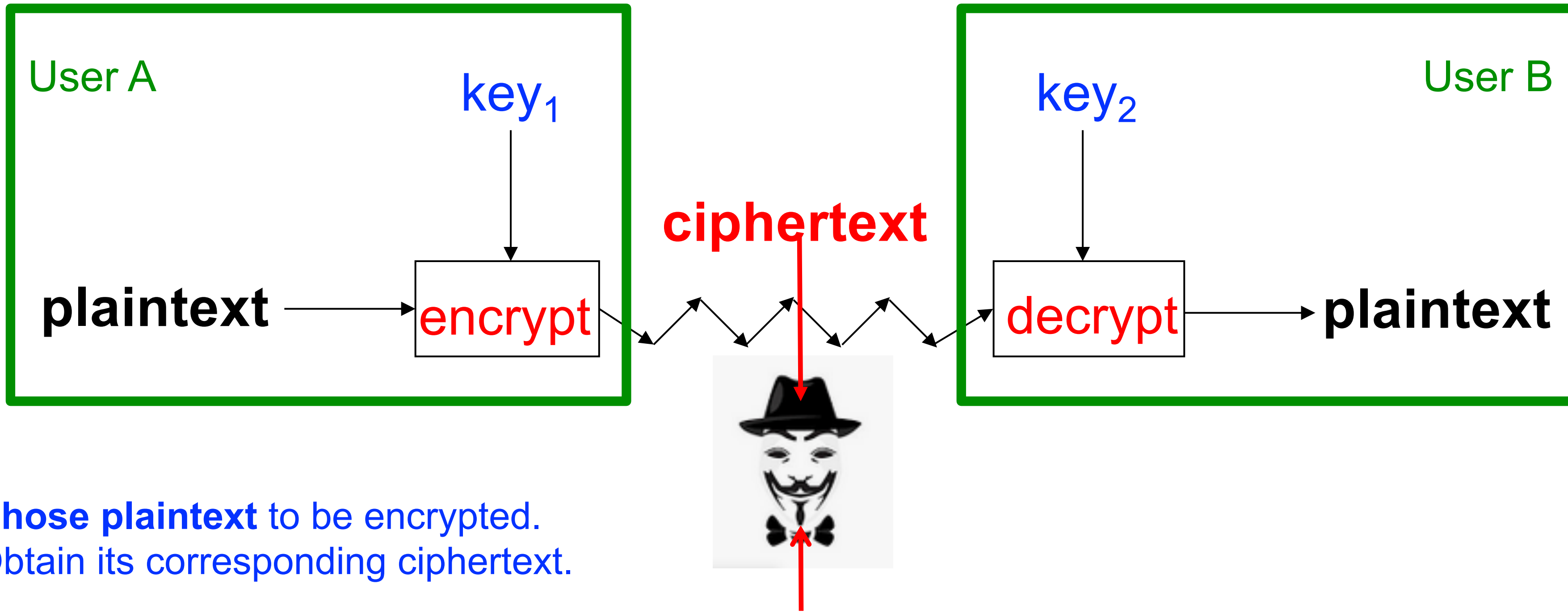
2. Known Plaintext Attack



Collect pairs of
plaintext and corresponding ciphertext

Given plaintext → Ciphertext of given plaintext → Given plaintext

3. Chosen Plaintext Attack



Chose plaintext to be encrypted.
Obtain its corresponding ciphertext.

Chosen plaintext → Ciphertext of chosen plaintext

4. Chosen Ciphertext Attack

User A

key_1

plaintext → encrypt

ciphertext

User B

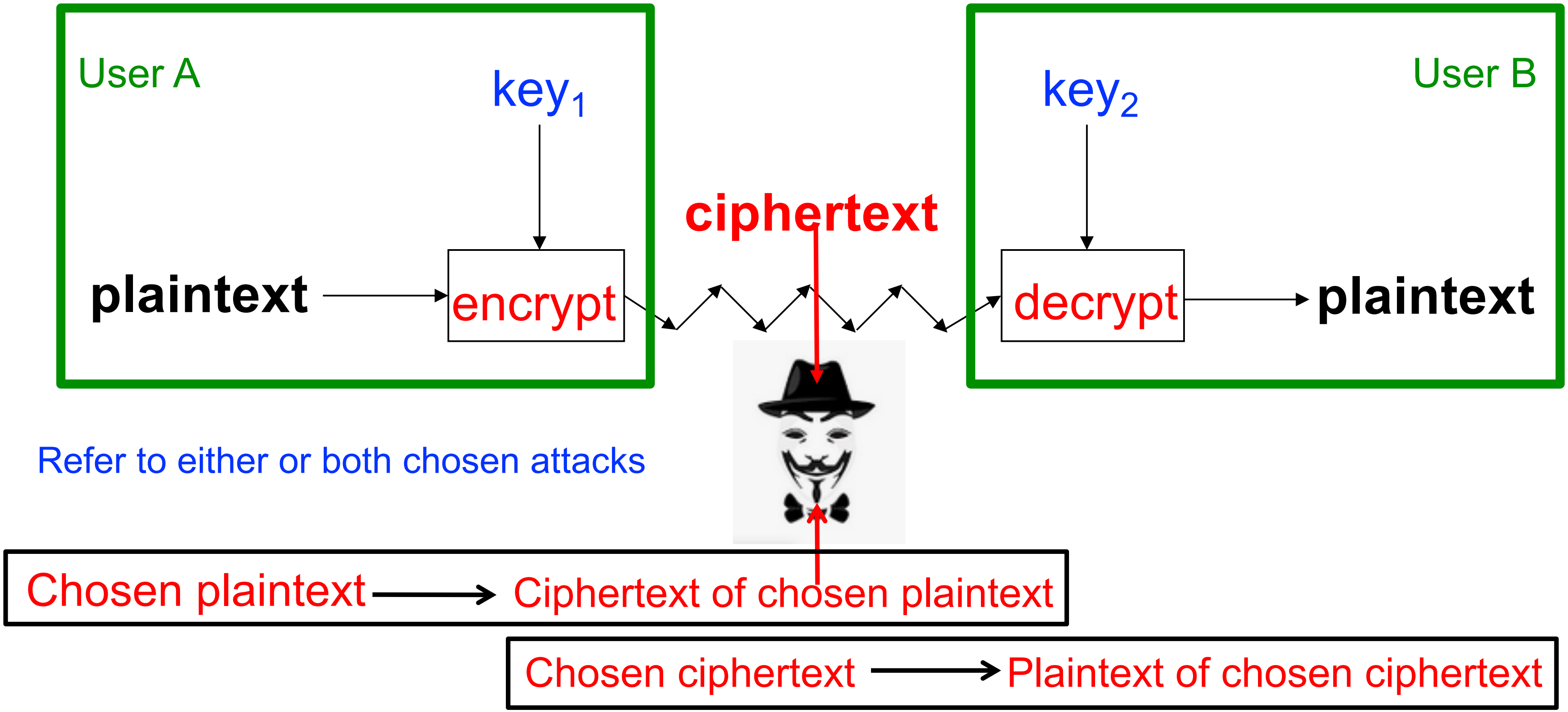
key_2

decrypt → plaintext

Chose a ciphertext.
Obtains its corresponding decrypted plaintext

Chosen ciphertext → Plaintext of chosen ciphertext

5. Chosen Text Attack



Refer to either or both chosen attacks

passive vs. active attacks

- **Passive**: adversary just receives some ciphertext
- **Active**: adversary can adaptively ask for encryption/decryption

Among all the attack scenarios, which are active attacks?

- A: Ciphertext only attack
- B: Known plaintext attack
- C: Chosen plaintext attack
- D: Chosen ciphertext attack
- E: Chosen text attack

passive vs. active attacks

- **Passive**: adversary just receives some ciphertext
- **Active**: adversary can adaptively ask for encryption/decryption

Among all the attack scenarios, which are active attacks?

- A: Ciphertext only attack
- B: Known plaintext attack
- **C: Chosen plaintext attack**
- **D: Chosen ciphertext attack**
- **E: Chosen text attack**

Historical ciphers

Simple Substitution Cipher

- Plaintext: fourscoreandsevenyearsago
- **Encryption:** substituting the letter of the alphabet **`n`** places ahead of the current letter
  - Shift by `n`
- Key: 3

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"

Caesar's Cipher Decryption

- Suppose we know a Caesar'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: EHJLQWKHDWWDFNQRZ

- Plaintext: begintheattacknow

Not-so-Simple Substitution

- Shift by n for some $n \in \{0, 1, 2, \ldots, 25\}$
- Then key is n
- Example: key $n = 13$

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	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

- This is also called ROT13

Cryptanalysis I: Try Them All

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

Simple Substitution – More Keys

- Is there a way to increase the size of keyspace for simple substitution?
  - 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!

Using previous machine(2^{40}), it takes around 9 million years to exhaustive key search!

Seems secure to me!

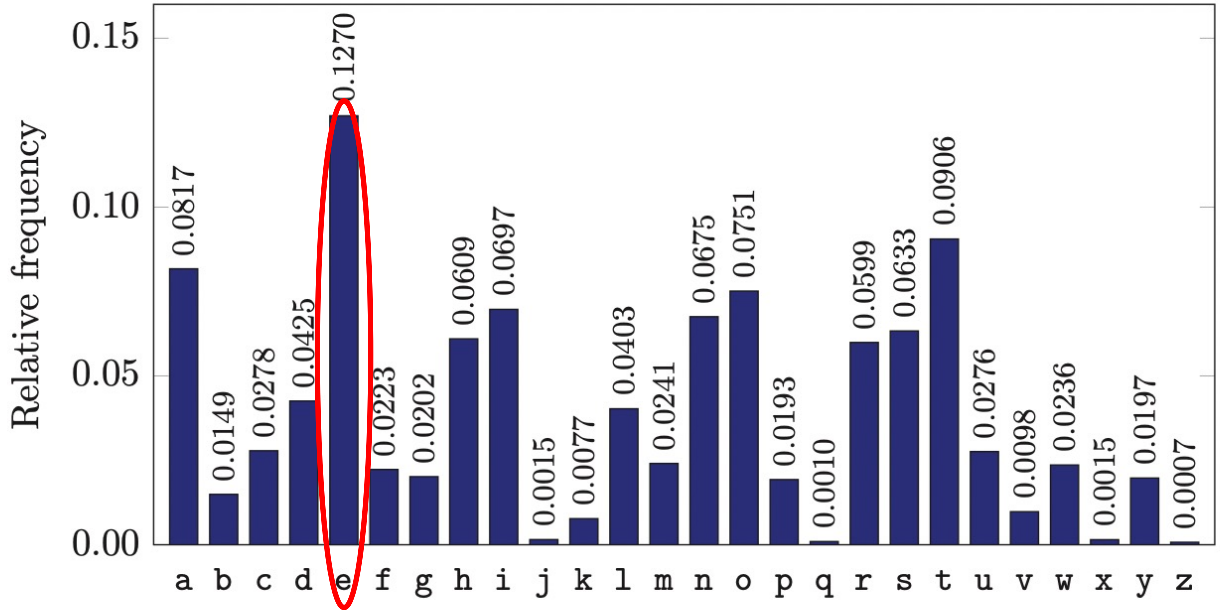
Cryptanalysis II: Be Clever

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

PBFPVYFBQXZTYFPBFEQJHDXXQVAPTPQJKTOYQWIPBVWLXTOXBTFXQWAX
BVCXQWAXFQJVWLEQNTOZQGGQLFXQWAKVWLXQWAEBIPBFXFQVXGTVJ
VWLBTPQWAEBFPBFHCVLXBQUFEVWLXGDPEQVPQGVPPBFTIXPFHXZHVF
AGFOTHFEFBQUFTDHZBQPOTHXTYFTODXQHFTDPTOGHFQPBQWAQJJTO
DXQHFOQPWTBDHHIXQVAPBFZQHCFWPFHPBFIPBQWKFABVYYDZBOTHPB
QPQJTQOTOGHFQAPBFEQJHDXXQVAVXEBQPEFZBVFOJIWFFACFCCFHQW
AUVWFLQHGFXVAFXQHFUFHILTTAVWAFFAWTEVOITDHFHFQAITIXPFHXAF
QHEFZQWGFLVWPTOFFA

Cryptanalysis II – Statistical Attack

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



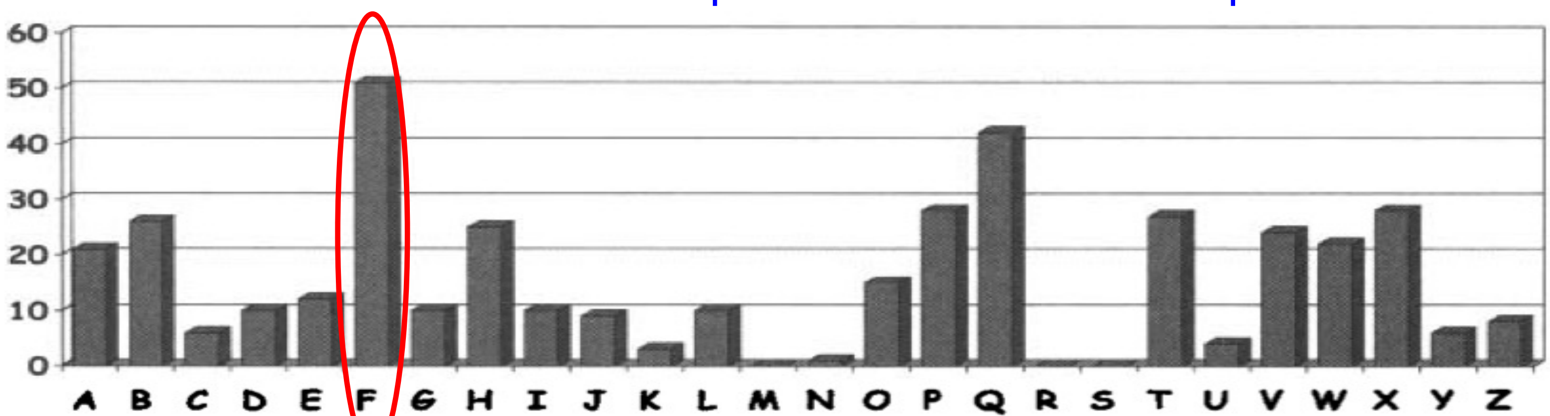
Cryptanalysis II – Statistical Attack

- Ciphertext:

PBFPVYFBQXZTYFPBFEQJHDXXQVAPTPQJKTOYQWIPBVWLXTOXBTFXQWAXBVCXQWAXF
QJVWLEQNTOZQGGQLFXQWAKVWLXQWAEBIPBFXFQVXGTVJVWLBTPQWAEBFPBFHCV
LXBQUFEVWLXGDPEQVPQGVPPBFTIXPFHXZHVFAGFOTHFEFBQUFTDHZBQPOTHXTYF
TODXQHFTDPTOGHFQPBQWAQJJTODXQHFOQPWTBDHHIXQVAPBFZQHCFWPFHPBFIP
BQWKFABVYYDZBOTHPBQPQJTQOTOGHFQAPBFEQJHDXXQVAVXEBQPEFZBVFOJIWFF
ACFCCFHQWAUVWFLQHGFXVAFXQHFUFHILTTAVWAFFAWTEVOITDHFHFQAITIXPFHXAF
QHEFZQWGFLVWPTOFFA

Ciphertext frequency counts:

Guess ‘F’ in ciphertext should be ‘e’ in plaintext



Cryptanalysis II – Statistical Attack

- Ciphertext:

PBFPVYFBQXZTYFPBFEQJHDXXQVAPTPQJKTOYQWIPBVWLXT
OXBTFXQWAXBVCXQWAXFQJVWLEQNTOZQGGQLFXQWAKVW
LXQWAEBIPBFXFQVXGTVJVWLBTPQWAEBFPBFHCVLXBQUFE
VWLXGDPEQVPQGVPPBFTIXPFHXZHVFAGFOTHFEFBQUFTDH
ZBQPOTHXTYFTODXQHFTDPTOGHFQPBQWAQJJTODXQHFOQ
PWTBDHHIXQVAPBFZQHCFWPFHPBFIPBQWKFABVYYDZBOTH
PBQPQJTQOTOGHFQAPBFEQJHDXXQVAVXEBQPEFZBVFOJIW
FFACFCCFHQWAUVWFLQHGFXVAFXQHFUFHILTTAVWAFFAWT
EVOITDHFHFQAITIXPFHXAFQHEFZQWGFLVWPTOFFA

‘F’ should be ‘E’
‘the’ is a popular starting word
‘P’ and ‘B’ relatively frequent in ciphertext
‘t’ and ‘h’ relatively frequent in plaintext

Guess → ‘P’ is ‘t’
‘B’ is ‘h’

Vigenere Cipher

- Simple substitution is ***monoalphabetic***
  - Each letter is always substitute by another fixed letter
    - 'a' is always substitute by 'D' in Cesar's Cipher
  - A fixed plaintext-ciphertext table can be generated
- Vigenere cipher is simple example of a ***polyalphabetic*** substitution
  - Caesars ciphers, based on a keyword
    - Shift based on keyword
- For example, keyword CAT indicates shift by 2, shift by 0, shift by 19
  - Then repeat as needed

Vigenere Example

- Suppose that we want to encrypt attackatdawn
- Encryption:

keyword:	CATCATCATCAT
plaintext:	attackatdawn
ciphertext:	ctmccdctwcwg

- Ciphertext is ctmccdctwcwg
- How to decrypt?
  - Reverse the process, shift back according to the keyword
- This obscures the statistical information from the ciphertext

Cryptanalysis III - Vigenere

Plaintext: `attackatdawn`
Keyword: `CATCATCATCAT`
Ciphertext: `ctmccdctwcwg`

- Suppose we know the **keyword length** and the ciphertext
  - Length is 3
- We can divide the ciphertext into 3 groups
  - **`ctmccdctwcwg`**
  - **`[C]cccc, [A]tctw, [T]mdwg`**
- The letter in the same group shift by the same ‘n’
  - The same keyword letter is used for that group
- This makes the Vigenere a multiple Caesar’s ciphers
- Decrypt each group with the 26 possible keys
  - get frequency of each decrypted group, compare it with the English frequency

BINGHAMTON UNIVERSITY STATE UNIVERSITY OF NEW YORK

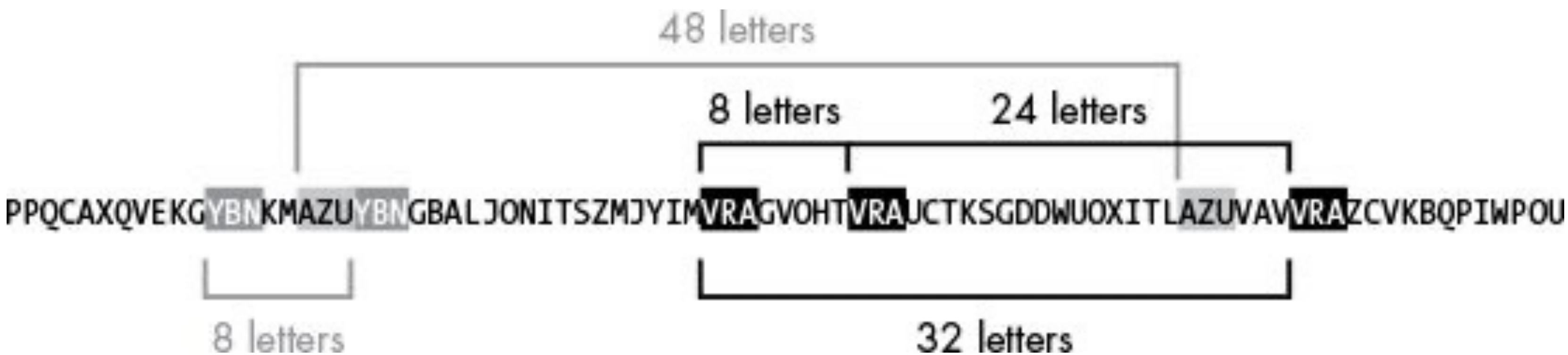
Cryptanalysis III - Vigenere

- How to get the keyword length just based on ciphertext?

Plaintext: `attackatdawn`
Keyword: `CATCATCATCAT`
Ciphertext: **`ct`**`mccd`**`ct`**`wcwg`

- Found repeat pattern in ciphertext
  - **ct**
- Guess the length based on pattern
  - 6
- Consider the factors of length as well
  - 2, 3
- Try each possible key length

Cryptanalysis III - Vigenere



Length	Factors
8	2, 4, 8
24	2, 4, 6, 8, 12, 24
32	2, 4, 8, 16
48	2, 4, 6, 8, 12, 24, 48

The key is most likely to be the most frequently occurring factors 2, 4, 8 in this example

Double Transposition

- Plaintext: attackxatxdawnx
  - 5 x 3 matrix

	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 $\Rightarrow$

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

Permute cols $\Rightarrow$

	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 is matrix size and permutations: (3, 5, 1, 4, 2) and (1, 3, 2)

Double Transposition - Decryption

- Ciphertext: xtawxnattxadakc
  - 5 x 3 matrix

	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

Undo cols (1, 3, 2) ⇒

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

Undo rows (3, 5, 1, 4, 2) ⇒

	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

- Plaintext: attackxatxdawnx
- Does not disguise the letters

XOR

- XOR (Exclusive OR) is a logical operation that outputs true only when the inputs differ
- Symbol: $\oplus$
- Truth table

Input A	Input B	Output
0	0	0
0	1	1
1	0	1
1	1	0

XOR properties

$A \oplus 0 = A,$

$A \oplus A = 0,$

$(A \oplus B) \oplus C = A \oplus (B \oplus C),$

$(B \oplus A) \oplus A = B \oplus 0 = B,$

- E.g., $1010 \oplus 1100 = 0110$

One-Time Pad

Alphabet

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

"xor"

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

Encryption

One-Time Pad

Alphabet

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

Decryption: Ciphertext $\oplus$ Key = Plaintext

Plaintext $\oplus$ Key $\oplus$ 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

Decryption

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…
  - Secure cipher
  - 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
- pad (key) is same size as message
  - Impractical for some real-world cases
- You can already distribute secure pad, why not distribute message itself instead?

Real-World One-Time Pad

- Project VENONA
  - Encrypted spy messages sent from U.S. to Moscow in 30's, 40's, and 50's
  - Nuclear etc.
  - Thousands of messages
- 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.

- "Enormous" == the atomic bomb

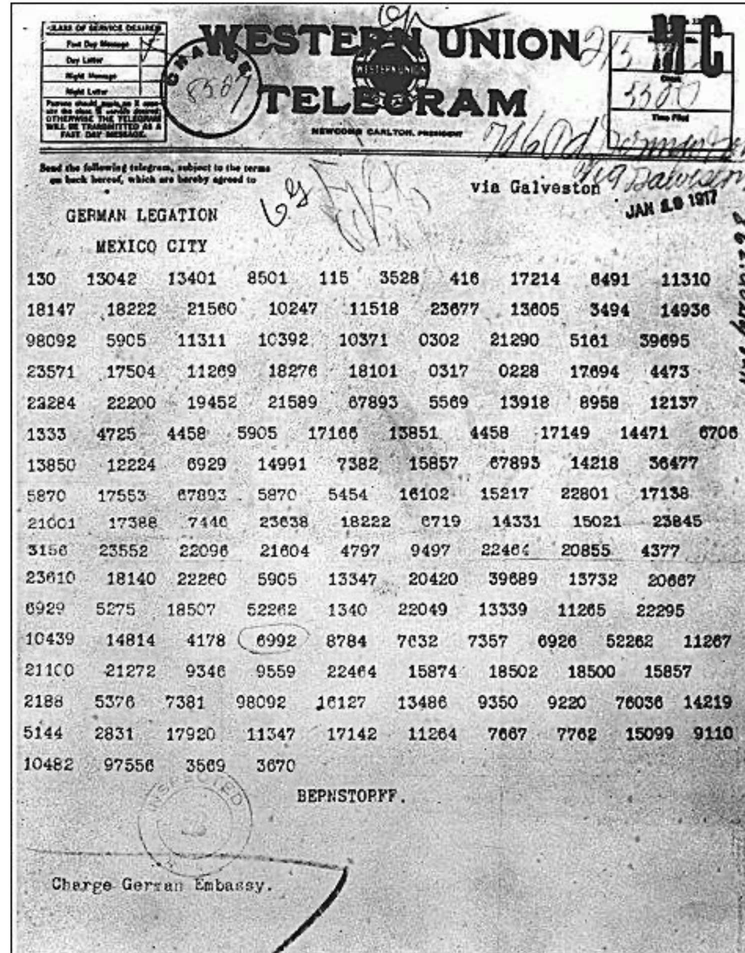
Codebook Cipher

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

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

Zimmerman Telegram

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


WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

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.

History behind Zimmerman Telegram

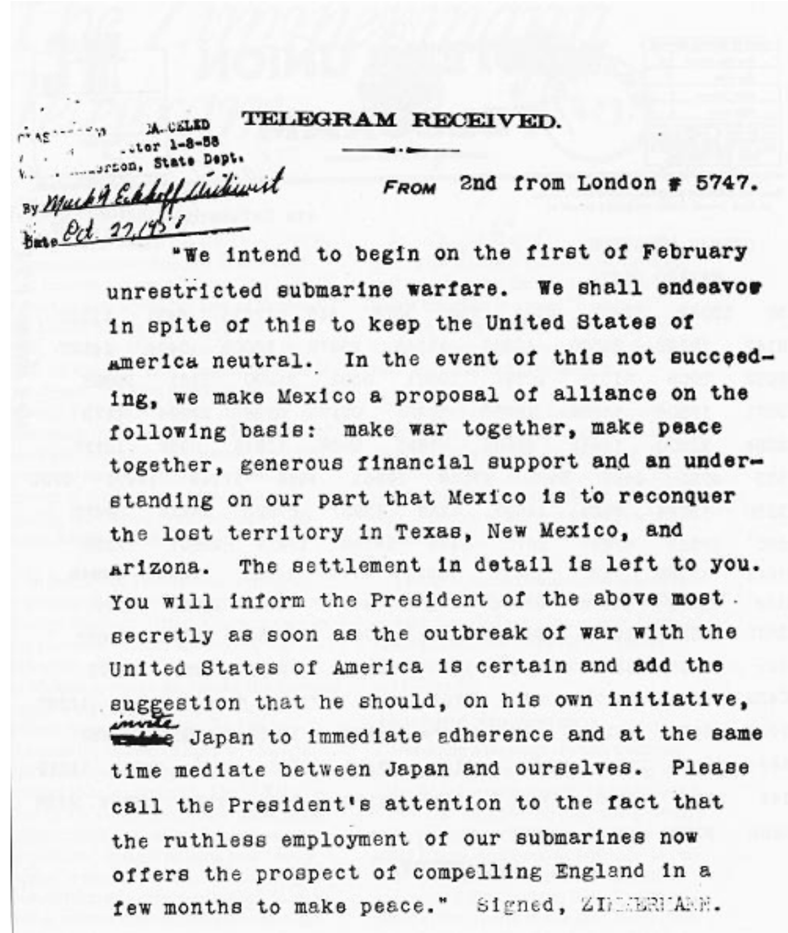
- Zimmerman (then the German Foreign Minister) sent an encrypted message to German Ambassador in Mexico City.

- Zimmermann told his ambassador that Germany should try to recruit Mexico as an ally to fight against the United States. The incentive for Mexico was that it would "reconquer the lost territory in Texas, New Mexico and Arizona."

- At that time, the British and French at war with German but US was neutral

Zimmerman Telegram Decrypted

- British had recovered partial codebook, then was able to fill in missing parts
- After the decrypted Zimmerman telegram was released to U.S., public opinion turned against Germany and, the U.S. declared war.



CANCELED
...ctor 1-8-58
...nderson, State Dept.
By Mark A Eckhoff Archivist
Date Oct. 22, 1958

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 - Additive

- Codebooks also (usually) use **additive**
- Additive — book of “random” numbers
- Procedure of using a codebook and addtive
  - Encrypt message with codebook
  - Then choose *position* in additive book
  - Add additives to get ciphertext
  - Send ciphertext and additive position
  - Recipient subtracts additives before decrypting
- Both the codebook and additive are needed for encryption and decryption
- Why use an additive sequence?
  - Reduce frequency analysis, increase the life of codebook

Codebook Cipher - Illustration

Additive codebook

Code
058
021
001
092
222
111
087
022
044

3

Original codebook

Word	Code
The	001
good	002
staff	003
dog	004
cat	005

Plaintext: good dog → 002 004

Random additive: 3

3 is sent in the clear at the start of transmission

Ciphertext: 094 226

What we have learned

- Basics of cryptography
  - Crypto terms
    - Crypto
    - Cryptography
    - Cryptanalysis
  - Kerckhoffs' principles

What we have learned

- Basics of cryptography
  - Crypto terms
  - Kerckhoffs’ principles
  - Shift crypto

What we have learned

- Basics of cryptography
  - Crypto terms
  - Kerckhoffs' principles
  - Shift crypto
  - Vegenere

What we have learned

- Basics of cryptography
  - Crypto terms
  - Kerckhoffs' principles
  - Shift crypto
  - Vegenere
  - Double transposition

What we have learned

- Basics of cryptography
  - Crypto terms
  - Kerckhoffs' principles
  - Shift crypto
  - Vegenere
  - Double transposition
  - One-time pad

Refresher: 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

BINGHAMTON UNIVERSITY STATE UNIVERSITY OF NEW YORK

Refresher: One-Time Pad, Decryption

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

Decryption: Ciphertext $\oplus$ 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

What we have learned

- Basics of cryptography
  - Crypto terms
  - Kerckhoffs' principles
  - Shift crypto
  - Double transposition
  - One-time pad
  - Codebook cipher

Codebook Cipher

Original codebook

Word	Code
The	001
good	002
staff	003
dog	004
cat	005

Additive codebook

Code
058
021
001
092
222
111
087
022
044

3

Plaintext: good dog → 002 004

Random additive: 3

Ciphertext: 094 226