Computer and Network Security

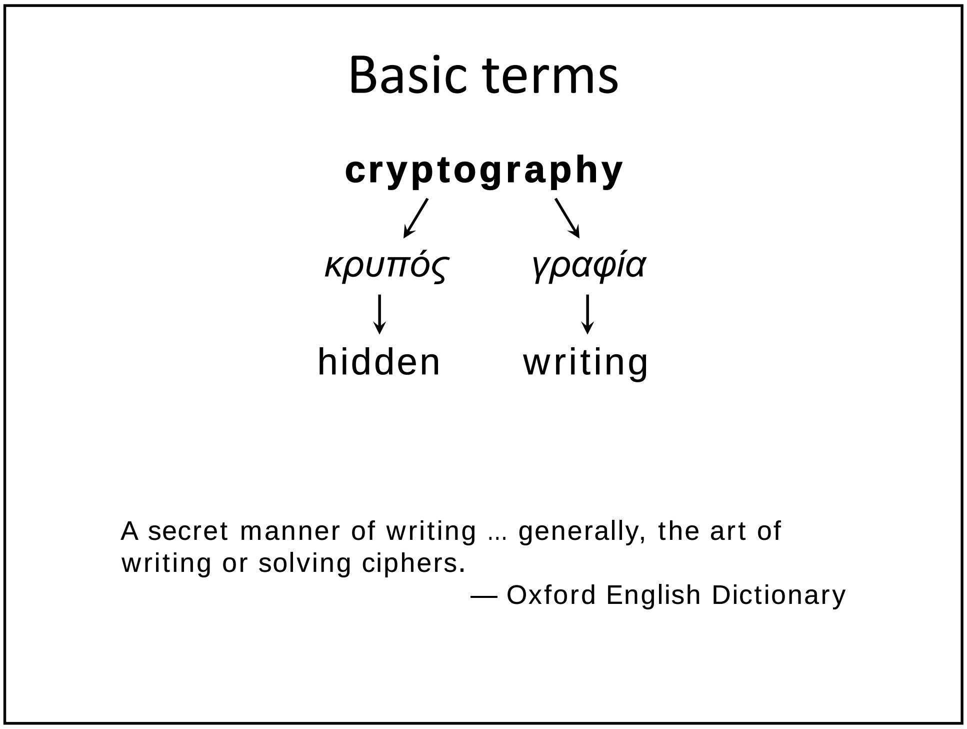
Lecture 2

Introduction to Cryptography

Acknowledgements:
Slides material taken from G. Tsudik, P. Krzyzanowski, D. Boneh, etc.

Outline

- Basic concepts
- Historical ciphers
- Cryptosystems
  - Definition
  - Security
  - Attacks



Basic terms

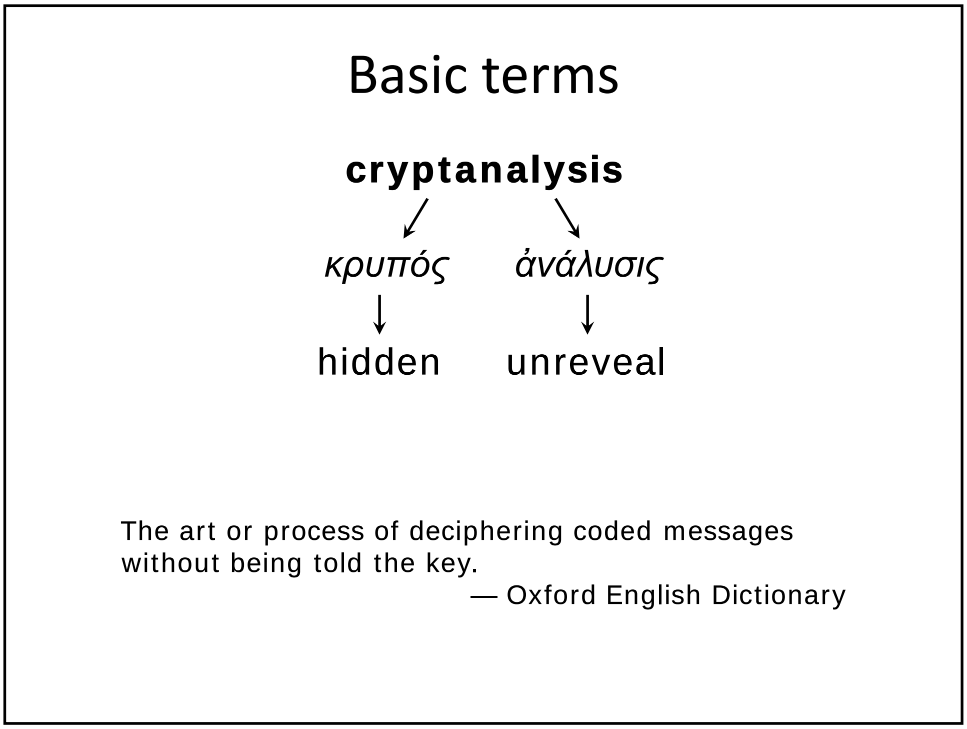
cryptography

κρυπός → hidden

γραφία → writing

A secret manner of writing … generally, the art of writing or solving ciphers.

— Oxford English Dictionary



Basic terms

cryptanalysis

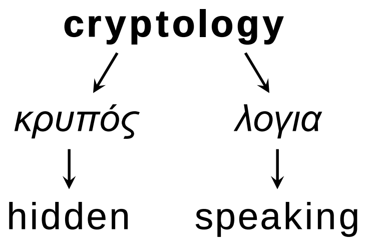
κρυπός → hidden

ἀνάλυσις → unreveal

The art or process of deciphering coded messages without being told the key.

— Oxford English Dictionary

Basic terms



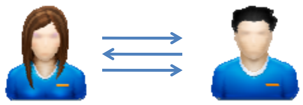
1967 D. Kahn, *Codebreakers* p. xvi, Cryptology is the science that embraces cryptography and cryptanalysis, but the term 'cryptology' sometimes loosely designates the entire dual field of both rendering signals secure and extracting information from them.

— Oxford English Dictionary

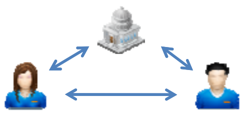
Cryptography – Different levels

- Algorithms: encryption, signatures, hashing, RNG

- Protocols (2 or more parties): key distribution, authentication, identification, login, payment, etc.



- Systems: electronic cash, secure file systems, VPNs, e-voting, etc.



- Attacks: on all the above

Cryptography – Applications

- Network, operating system security
- Protect Internet, phone, satellite communications
- Electronic payments (e-commerce)
- Database security
- Software/content piracy protection
- Pay TV
- Military communications
- Voting

Open Vs. Closed design

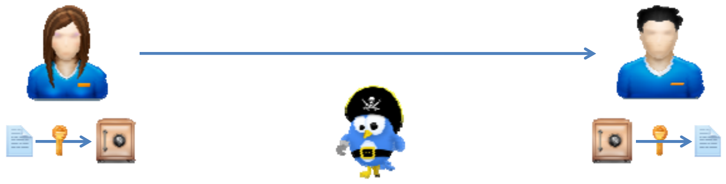
- **Open design**: algorithm, protocol, system design are public information
  - Only key(s) are kept secret

OpenSSH

- **Closed design:** as much information as possible is kept secret

DIGITAL+

The core issue
How to communicate securely?



Easy?

Main headache

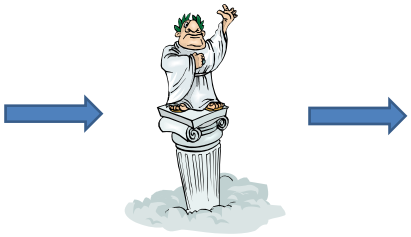
- Effective, yet unobtrusive
  - Should work for average users
- Security is not a service
  - Enabler
  - Inhibitor
  - Implies overhead

Cryptography
Older than you might think

- Most Computer Science sub-fields are fairly new:
  - Graphics, compilers, software, CSCW, etc.
- And a few are quite old:
  - Database, networking, etc.
- Cryptography is the oldest!

Caesar's cipher

Homo
Hominem
Lupus!



Krpr
Krplqhp
Oxsxv!

- Earliest documented military use of cryptography
  - Julius Caesar 60 B.C.
- Shift cipher
  - each letter replaced by one **k** positions away modulo alphabet size
  - **k** = shift value = key

ENIGMA

- Poly-alphabetic substitution cipher
- Invented at the end of WWI
  - Used in WWII by Germans
- Too bad it was cryptanalysis years before by Polish cryptologist

Historical Ciphers

- Shift (e.g., Caesar): $\mathrm{Enc}_{k}(x) = x + k \bmod 26$
- Affine: $\mathrm{Enc}_{k1,k2}(x) = k1 * x + k2 \bmod 26$
- Substitution: $\mathrm{Enc}_{perm}(x) = perm(x)$
- Vernam: one-time pad (OTP)

Shift Cipher (Caesar’s Chiper)

Encryption

W	E	W	I	L	L	M	E	E	T	A	T	M	I	D	N	I	G	H	T
22	4	22	8	11	11	12	4	4	19	0	19	12	8	3	13	8	6	7	19

+ 11 mod 26

7	15	7	19	22	22	23	15	15	4	11	4	23	19	14	24	19	17	18	4
H	P	H	T	W	W	X	P	P	E	L	E	X	T	O	Y	T	R	S	E

Decryption

- 11 mod 26

22	4	22	8	11	11	12	4	4	19	0	19	12	8	3	13	8	6	7	19
W	E	W	I	L	L	M	E	E	T	A	T	M	I	D	N	I	G	H	T

$\mathrm{Enc}_k(x) = x+k \bmod 26$

$\mathrm{Dec}_k(x) = x- k \bmod 26$

K = 11

- How many keys?
- How many trials to find the key?

Substitution Cipher

Key

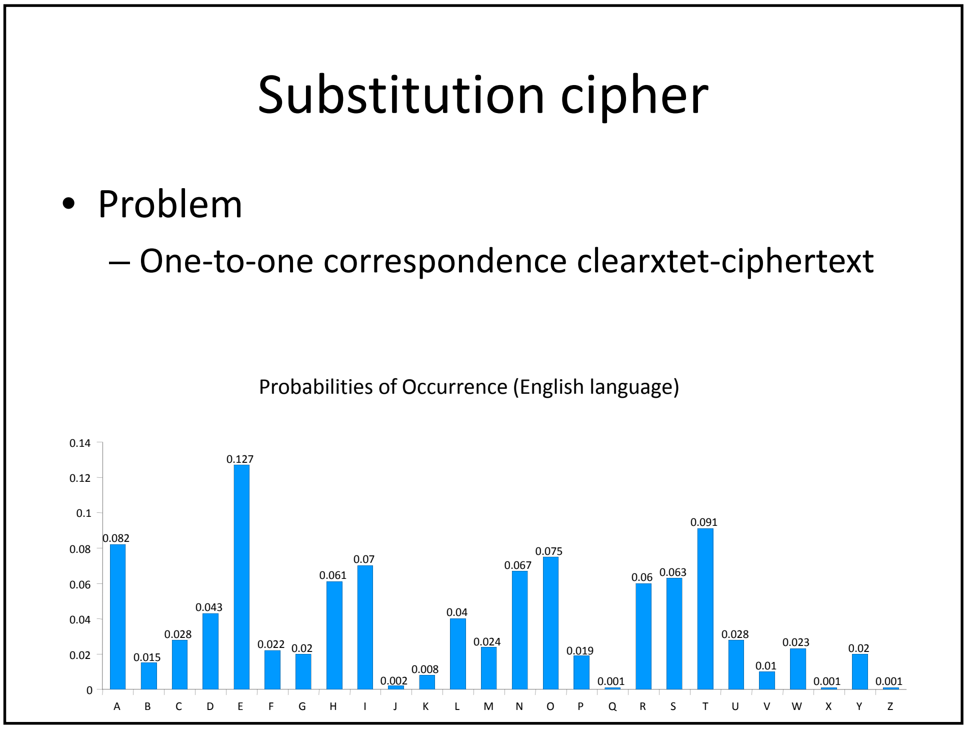
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	W	Z
X	N	Y	A	H	P	O	G	Z	Q	W	B	T	S	F	L	R	C	V	M	U	E	K	J	D	I

←Encryption

			W	E	W	I	L	L	M	E	E	T	A	T	M	I	D	N	I	G	H	T			
			K	H	K	Z	B	B	T	H	H	M	X	M	T	Z	A	S	Z	O	G	M			

Decryption→

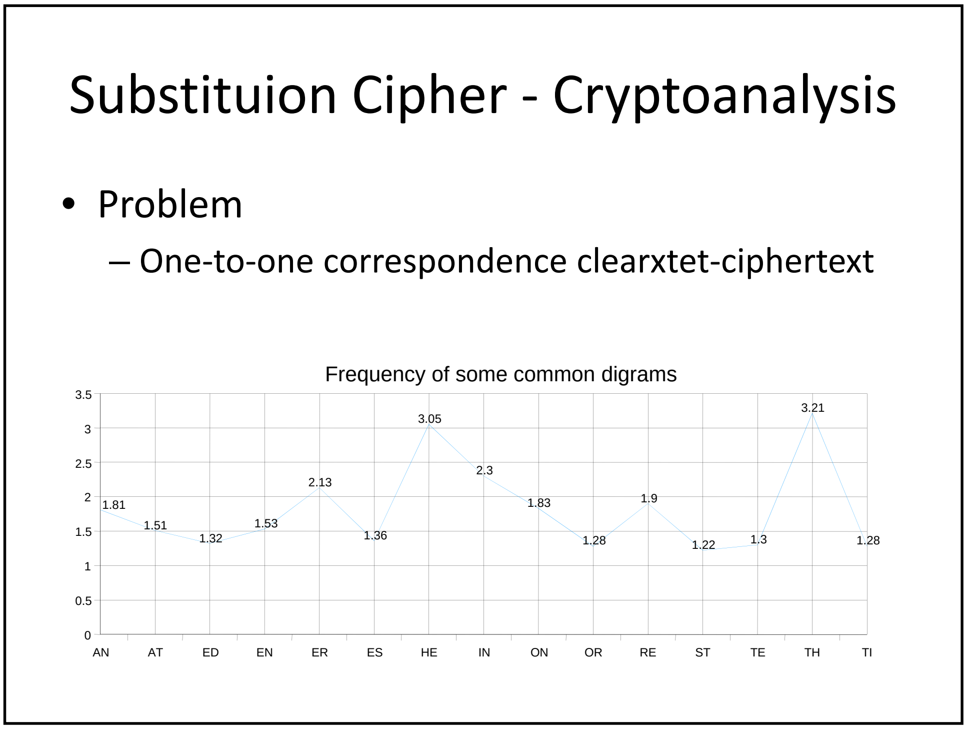
- How many keys?
- How many trials to find the key?



Substitution cipher

- Problem
  - One-to-one correspondence clearxtet-ciphertext

Probabilities of Occurrence (English language)



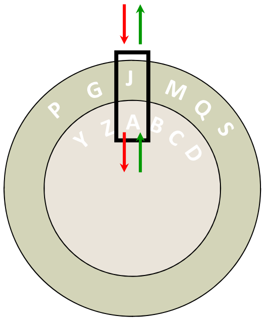
Substituion Cipher - Cryptoanalysis

- Problem
  - One-to-one correspondence clearxtet-ciphertext

Frequency of some common digrams

Poly-alphabetic ciphers

- Designed to thwart frequency analysis techniques
  - Different ciphertext symbols can represent the same plaintext symbol
  - One-to-many relationship between letter and substitute
- Aliberti's cipher (1466)
  - Two disks
  - Line up predetermined letter on inner disk with outer disk
  - Plaintext on inner → ciphertext on outer
  - After n symbols, the disk is rotated to a new alignment



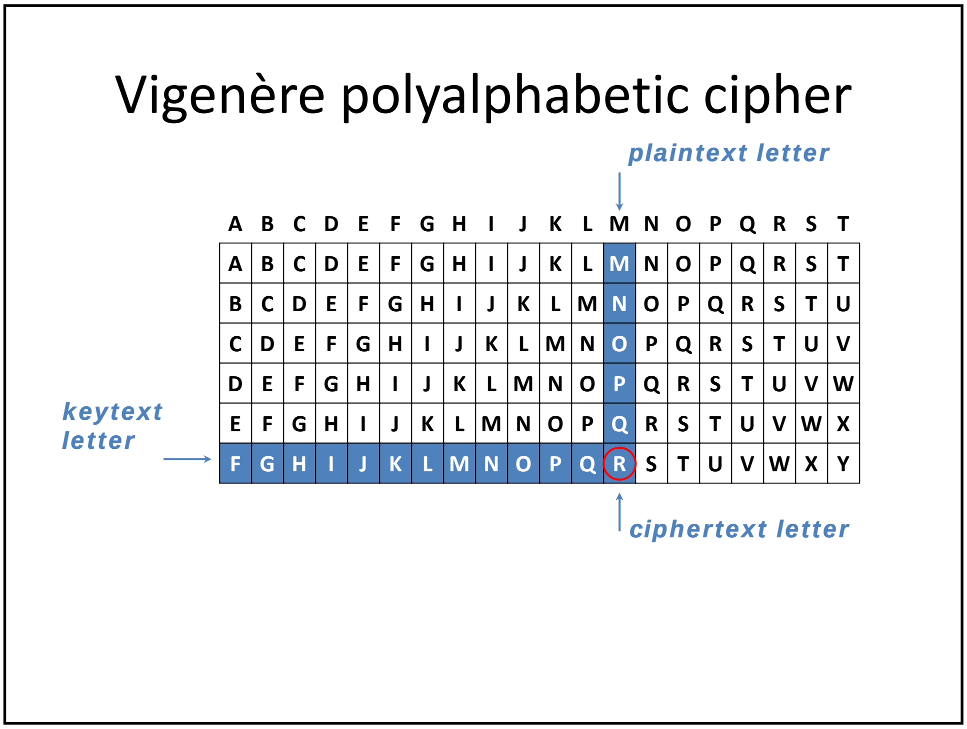
encrypt: A→J
decrypt: J →A

Vigenère poly-alphabetic cipher

- Blaise de Vigenère, court of Henry III of France, 1518
- Use **table+key** word to encipher a message
- Repeat keyword over text: (e.g., keyword = FACE)

```
FA CEF ACE FACEF ....
MY CAT HAS FLEAS ....
```

- Encryption → find intersection:
  - row = keyword letter
  - column = plaintext letter
- Decryption
  - column = keyword letter
  - search for intersection = ciphertext letter
- message is encrypted with as many substitution ciphers as there are letters in the keyword



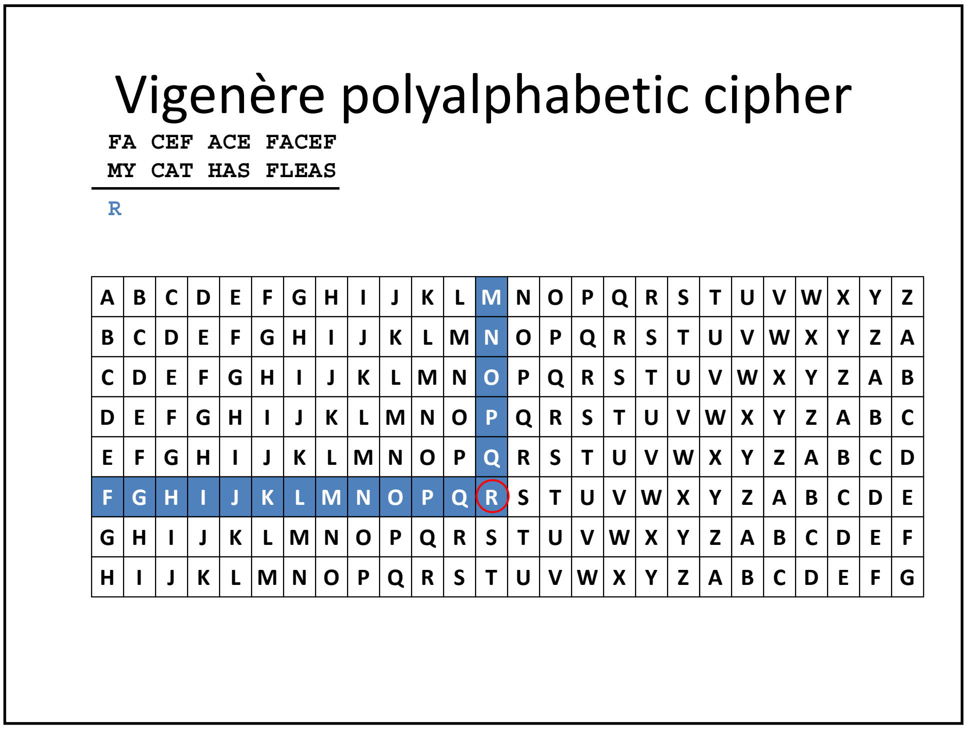
Vigenère polyalphabetic cipher

plaintext letter

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

keytext letter

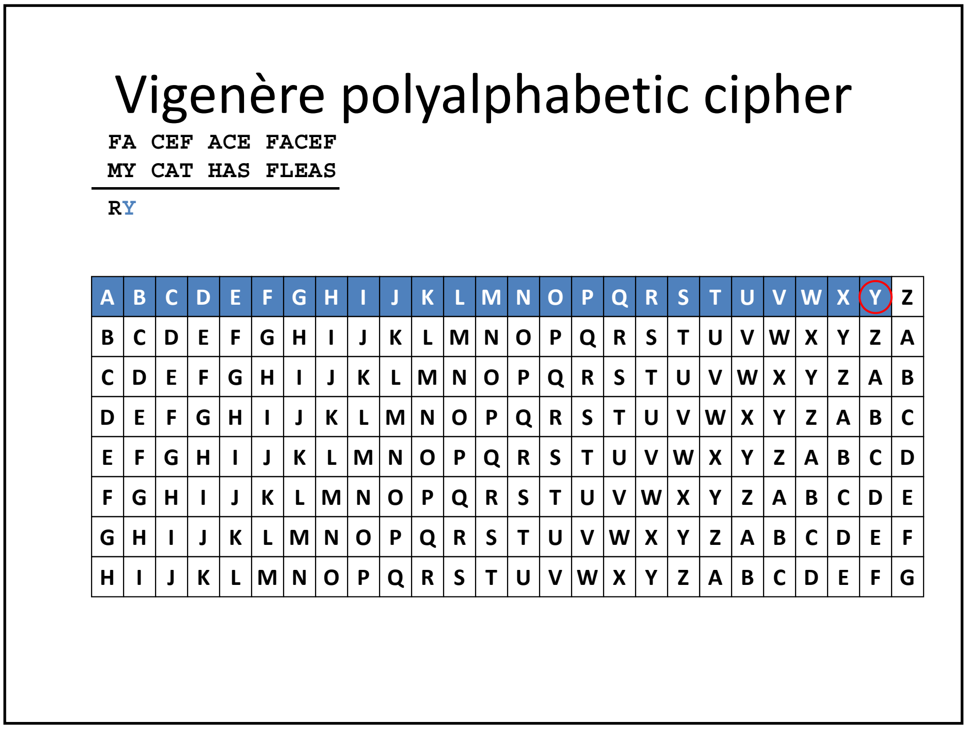
ciphertext letter



Vigenère polyalphabetic cipher

```
FA CEF ACE FACEF
MY CAT HAS FLEAS
R
```

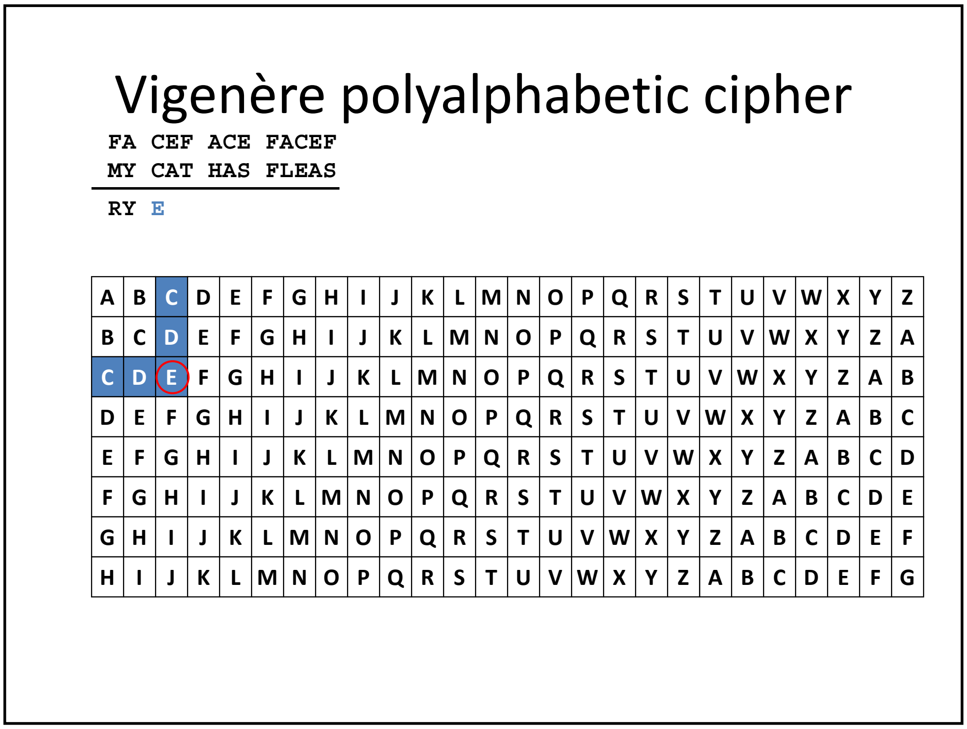
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z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



Vigenère polyalphabetic cipher

```
FA CEF ACE FACEF
MY CAT HAS FLEAS
RY
```

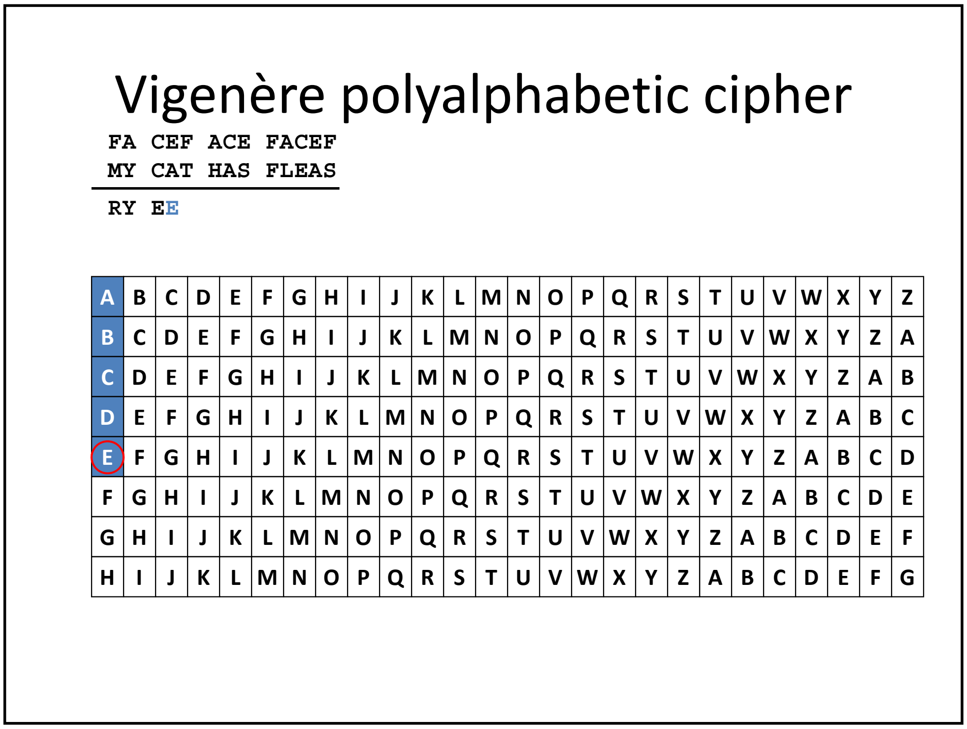
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z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



Vigenère polyalphabetic cipher

```
FA CEF ACE FACEF
MY CAT HAS FLEAS
RY E
```

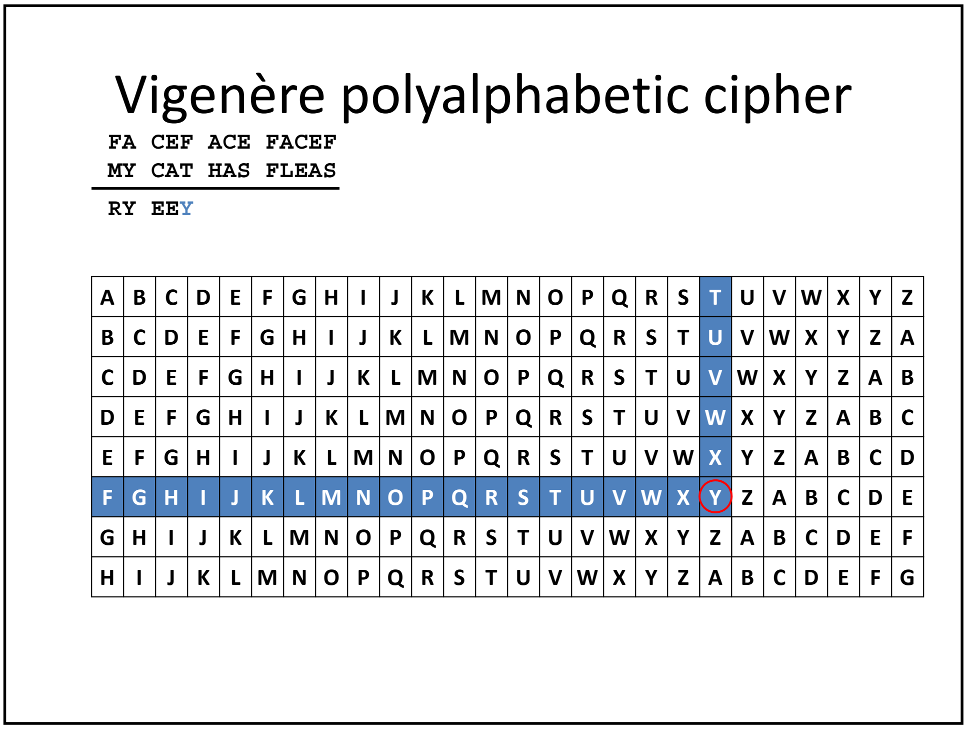
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z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



Vigenère polyalphabetic cipher

```
FA CEF ACE FACEF
MY CAT HAS FLEAS
RY EE
```

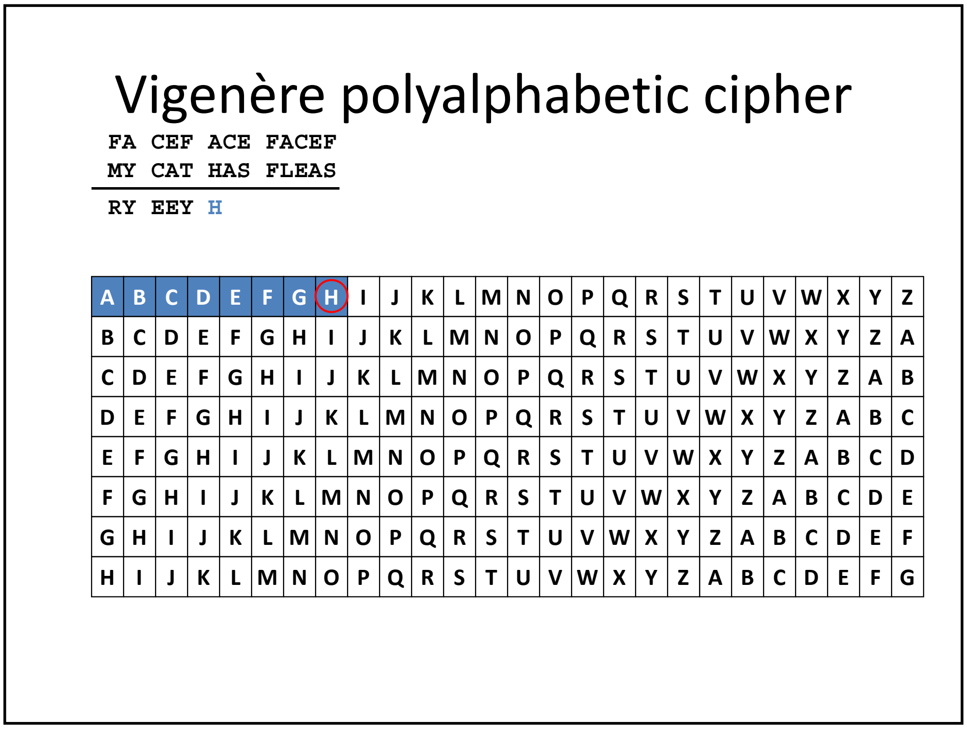
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z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



Vigenère polyalphabetic cipher

```
FA CEF ACE FACEF
MY CAT HAS FLEAS
RY EEY
```

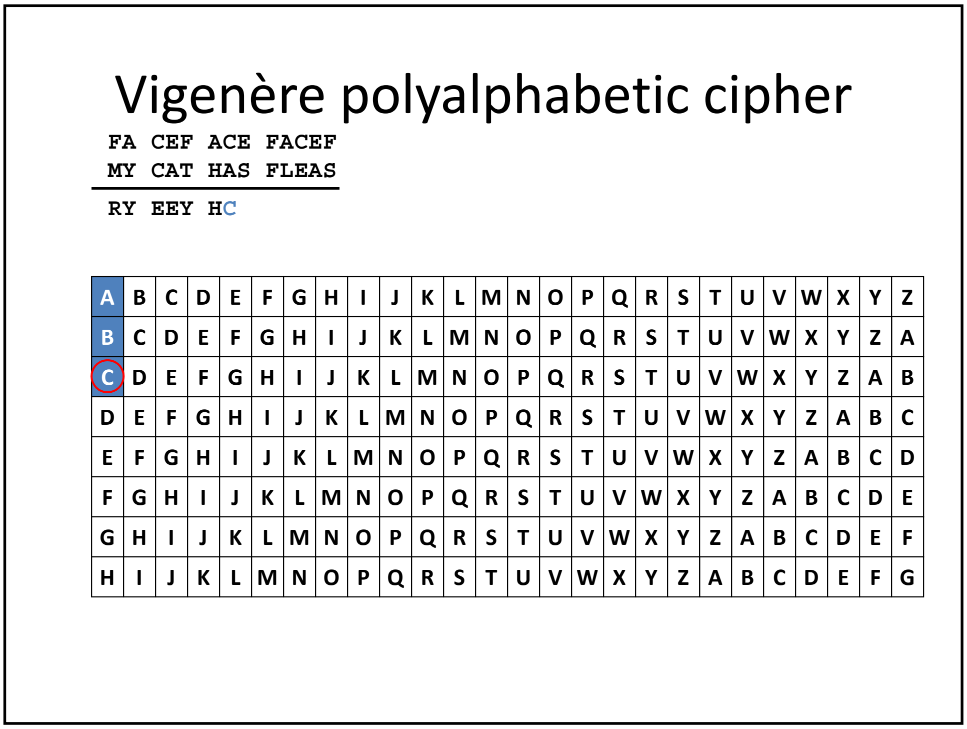
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z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



Vigenère polyalphabetic cipher

```
FA CEF ACE FACEF
MY CAT HAS FLEAS
RY EEY H
```

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	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	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	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	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	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	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	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



Vigenère polyalphabetic cipher

```
FA CEF ACE FACEF
MY CAT HAS FLEAS
RY EEY HC
```

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	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	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	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	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	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	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	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

Vigenère polyalphabetic cipher

```
FA CEF ACE FACEF
MY CAT HAS FLEAS
RY EEY HCW
```

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	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	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	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	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	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	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	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

Vigenère polyalphabetic cipher

```
FA CEF ACE FACEF
MY CAT HAS FLEAS
RY EEY HCW K
```

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	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	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	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	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	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	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	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

Vigenère polyalphabetic cipher

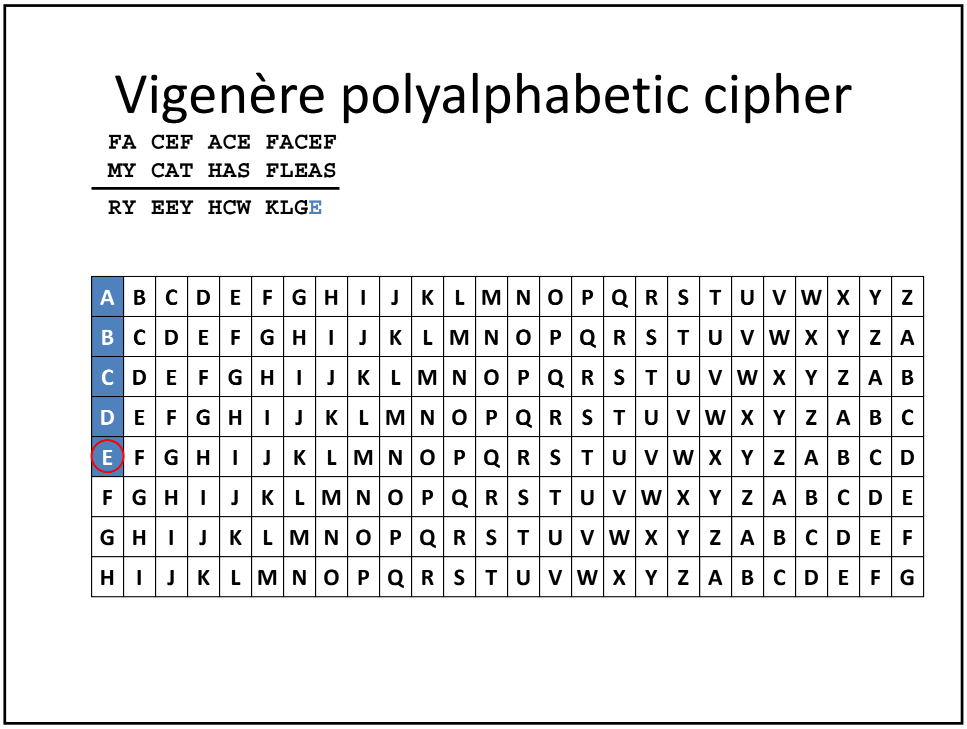
```
FA CEF ACE FACEF
MY CAT HAS FLEAS
RY EEY HCW KL
```

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	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	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	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	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	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	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	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

Vigenère polyalphabetic cipher

```
FA CEF ACE FACEF
MY CAT HAS FLEAS
RY EEY HCW KLG
```

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	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	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	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	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	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	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	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

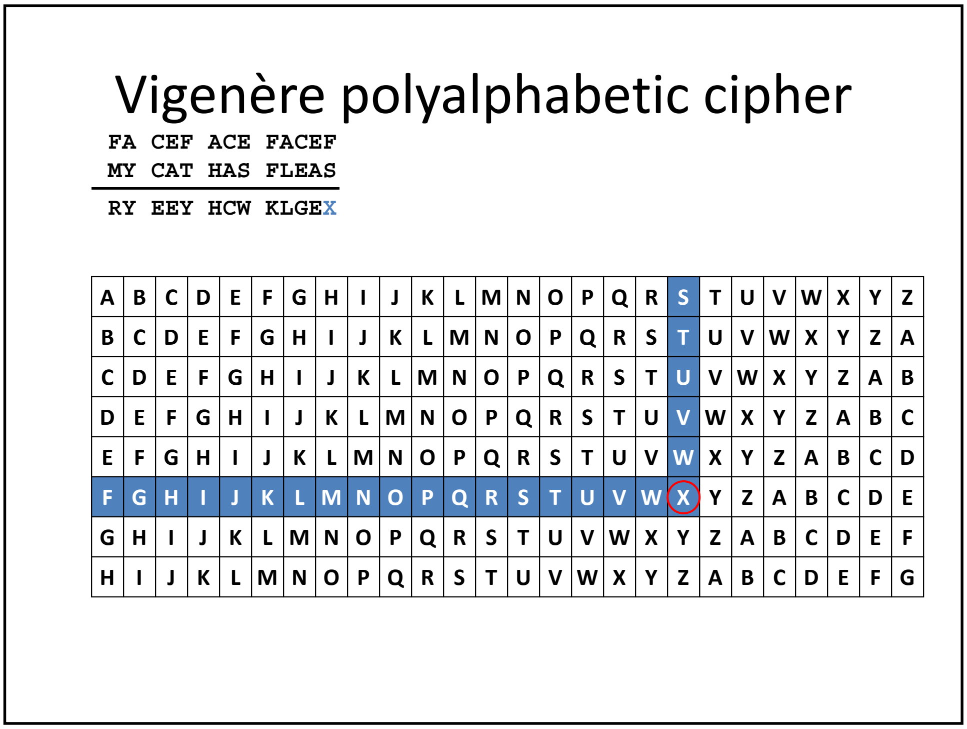


Vigenère polyalphabetic cipher

FA CEF ACE FACEF
MY CAT HAS FLEAS

RY EEY HCW KLGE

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	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	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	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	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	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	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	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



Vigenère polyalphabetic cipher

FA CEF ACE FACEF
MY CAT HAS FLEAS

RY EEY HCW KLGEX

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	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	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	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	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	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	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	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

Vernam Cipher

- One Time Pad (OTP)
- World's best cipher!

$\mathbf{c_i = p_i \oplus k_i}$

$\mathbf{p_i = c_i \oplus k_i}$

- Plaintext: $p_0,\ldots,p_{n-1}$
- OTP: $k_0,\ldots,k_{n-1}$
- Ciphertext: $c_0,\ldots,c_{n-1}$

Encryption

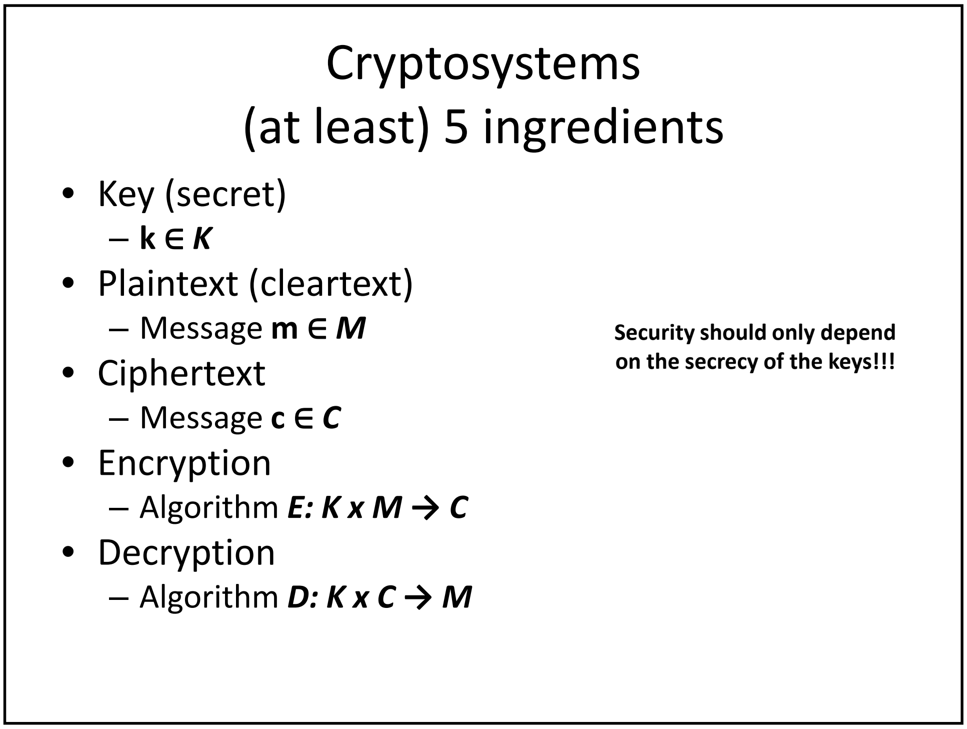
Plaintext	1 1 0 1 1 0 1 0 1
OTP	0 1 0 0 1 0 0 1 0
Ciphertext	1 0 0 1 0 0 1 1 1

Decryption

Ciphertext	1 0 0 1 0 0 1 1 1
OTP	0 1 0 0 1 0 0 1 0
Plaintext	1 1 0 1 1 0 1 0 1

Vernam Cipher – what's wrong?

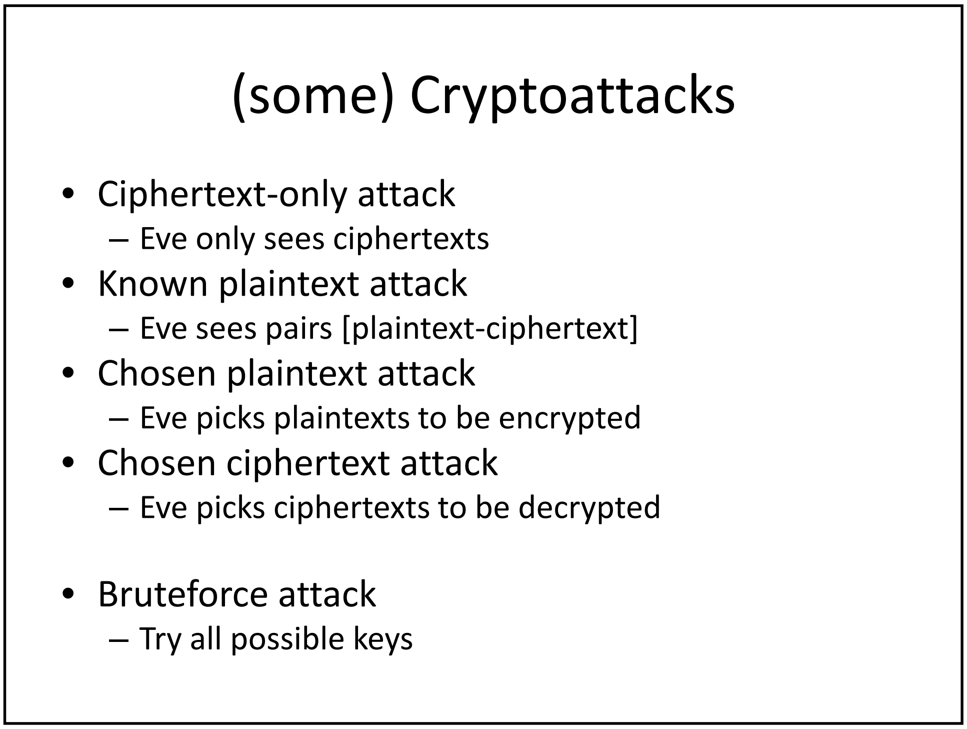
- Offers perfect (information-theoretic) security but…
- How long the OTP keystream should be?
- How do Alice and Bob exchange the OTP keystream?



Cryptosystems (at least) 5 ingredients

- Key (secret)
  - $\mathbf{k} \in \boldsymbol{K}$
- Plaintext (cleartext)
  - Message $\mathbf{m} \in \boldsymbol{M}$
- Ciphertext
  - Message $\mathbf{c} \in \boldsymbol{C}$
- Encryption
  - Algorithm $\boldsymbol{E: K \text{ x } M \rightarrow C}$
- Decryption
  - Algorithm $\boldsymbol{D: K \text{ x } C \rightarrow M}$

Security should only depend on the secrecy of the keys!!!



(some) Cryptoattacks

- Ciphertext-only attack
  - Eve only sees ciphertexts
- Known plaintext attack
  - Eve sees pairs [plaintext-ciphertext]
- Chosen plaintext attack
  - Eve picks plaintexts to be encrypted
- Chosen ciphertext attack
  - Eve picks ciphertexts to be decrypted

- Bruteforce attack
  - Try all possible keys

Bruteforce attack – average time

Key Size (bits)	Number of Alternative Keys	Time required at 10^6 Decr/µs
32	$2^{32} = 4.3 \times 10^{9}$	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	10 hours
128	$2^{128} = 3.4 \times 10^{38}$	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	5.9×10^{30} years

Types of attainable security

- Perfect, unconditional or information-theoretic:
  - security is evident free of any assumptions
- Provable:
  - security can be shown to be based on some common (often unproven) assumptions
    - Discrete logarithm problem
      - Given p prime and $Z_p^*=\{1,\ldots,p-1\}$
      - Find x s.t. $a^x = b \mod p$
- Ad hoc:
  - the security seems good…

Computational Security

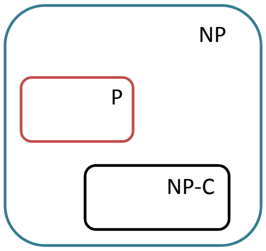
- Cost of breaking it (via brute force) exceeds the value of the encrypted information; or
- Time required to break it exceeds useful lifetime of the encrypted information

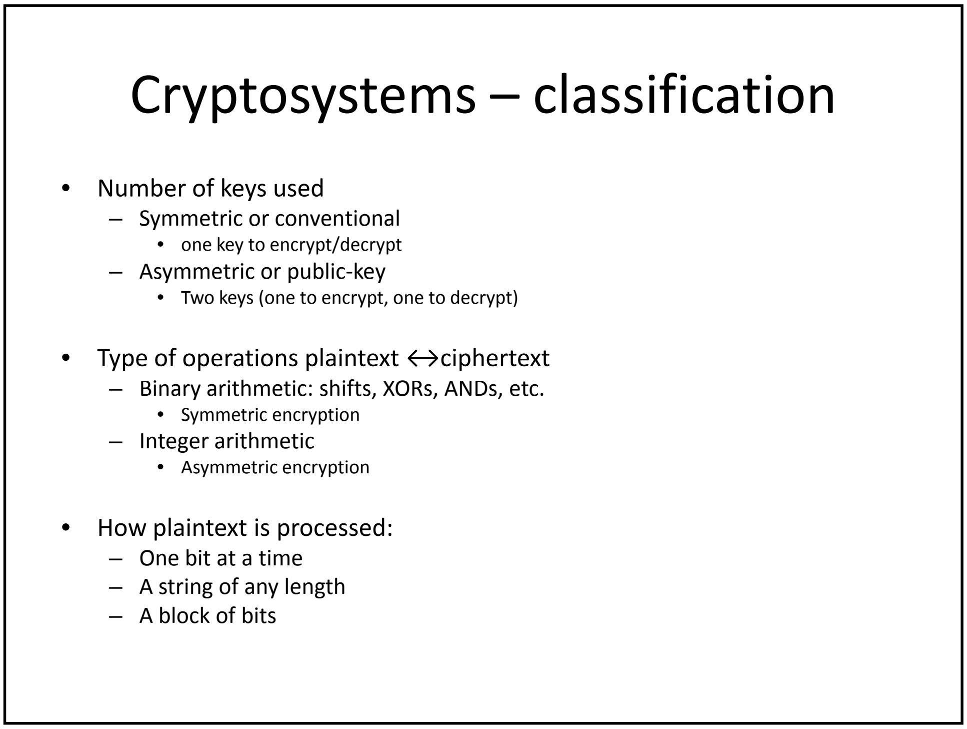
- Most modern schemes are considered computationally secure
  - rely on very large key-space

- Most advanced schemes rely on lack of knowledge of effective algorithms for certain hard problems
  - E.g., factorization, discrete logarithm, etc.

Complexity recap

- **P**: problems that can be solved in polynomial time
  - Find a solution can be done *efficiently*
- **NP**: broad set of problems that includes P
  - *Efficient* answer verification
  - Find a solution is not always *efficient*
- **NP-C**: believed-to-be-hard decision problems
  - If we can handle one, we can handle all problems in NP
- Examples:
  - Discrete log are in NP, not know if in NP-C or in P
  - Primality testing was recently shown to be in P
  - Knapsack is in NP-C





Cryptosystems – classification

- Number of keys used
  - Symmetric or conventional
    - one key to encrypt/decrypt
  - Asymmetric or public-key
    - Two keys (one to encrypt, one to decrypt)
- Type of operations plaintext ↔ciphertext
  - Binary arithmetic: shifts, XORs, ANDs, etc.
    - Symmetric encryption
  - Integer arithmetic
    - Asymmetric encryption
- How plaintext is processed:
  - One bit at a time
  - A string of any length
  - A block of bits