WEEK 2A

ENCRYPTION BASICS

SE 4472 - Information Security

Western Engineering

WHISPER LAB

ENCRYPTION

What is encryption?

TERMINOLOGY

01 PLAINTEXT

Unencrypted information

HELLO WORLD

02 CIPHERTEXT

Encrypted information

JJWNTY6TJKB

03 KEY

Secret to transform between plaintext and ciphertext

```
b1946ac92492d234
7c6235b4d2611184
```

TERMINOLOGY

04 PLAINTEXT SPACE

Set of valid plaintexts

05 CIPHERTEXT SPACE

Set of valid ciphertexts

01

10

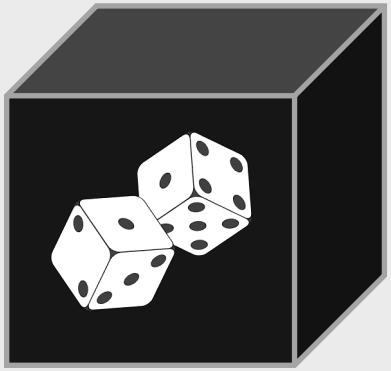
06 KEY SPACE

Set of valid keys

KEY GENERATION

KEY LENGTH

SECURITY PARAMETER



RANDOMIZED ALGORITHM

KEY

ENCRYPTION AND DECRYPTION

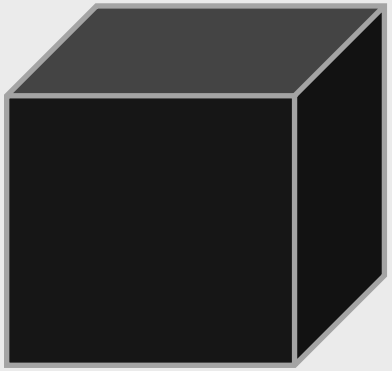
ENCRYPTION

PLAINTEXT

ELEMENT OF PLAINTEXT SPACE

KEY

ELEMENT OF KEY SPACE



CIPHERTEXT

ELEMENT OF CIPHERTEXT SPACE

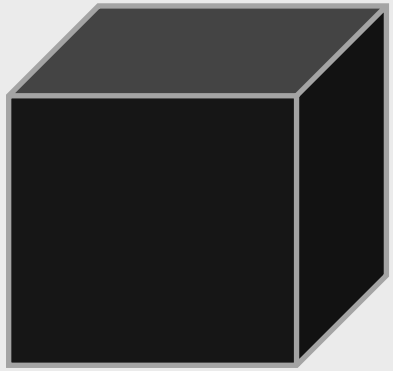
DECRYPTION

CIPHERTEXT

ELEMENT OF CIPHERTEXT SPACE

KEY

ELEMENT OF KEY SPACE



PLAINTEXT

ELEMENT OF PLAINTEXT SPACE

PROPERTIES

EFFICIENT

Encryption, decryption and key generation are efficiently computable

UNIQUE DECRYPTION

Decrypting the encryption of a message always returns the original message

CONFIDENTIAL

Difficult to extract information about the plaintext without the key

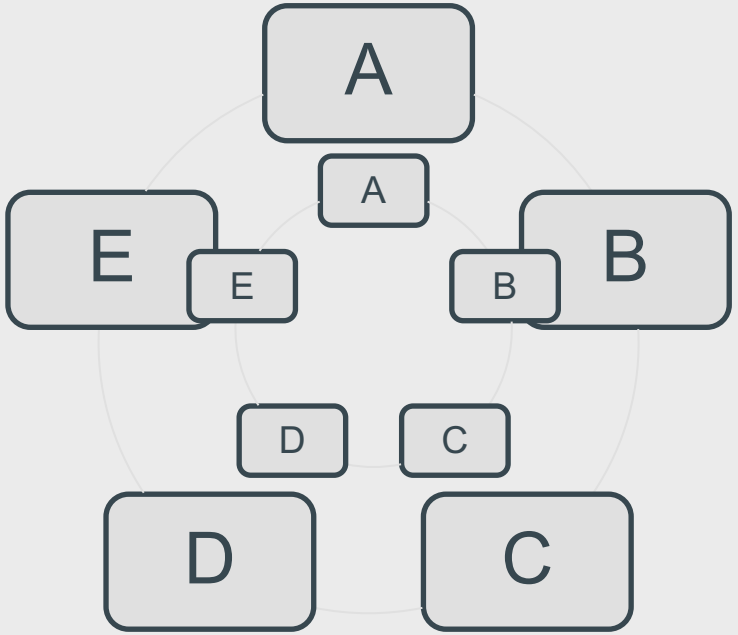
SECURE

It should be hard to guess the key, even with knowledge of a plaintext/ciphertext pair

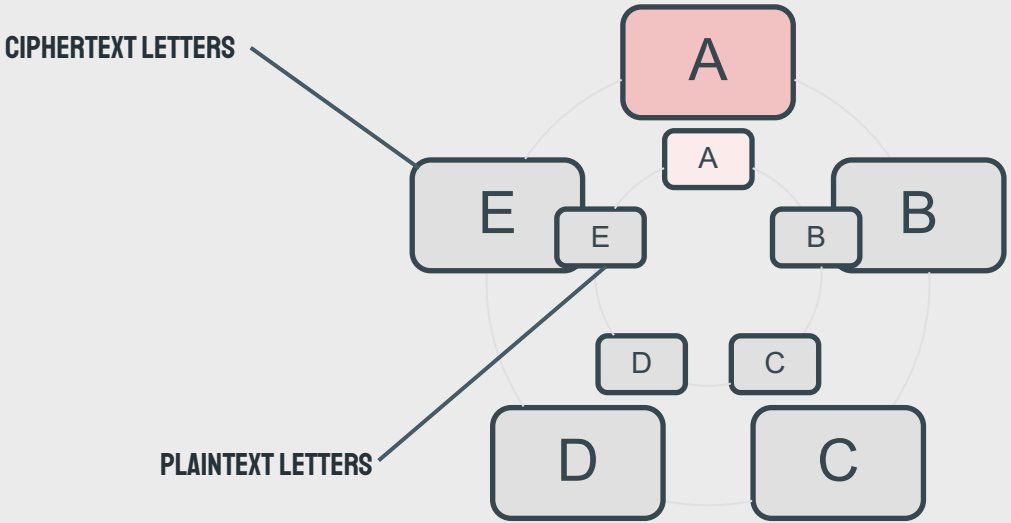
CLASSICAL CIPHERS

SUBSTITUTION CIPHERS

SWAPPING ONE LETTER FOR ANOTHER

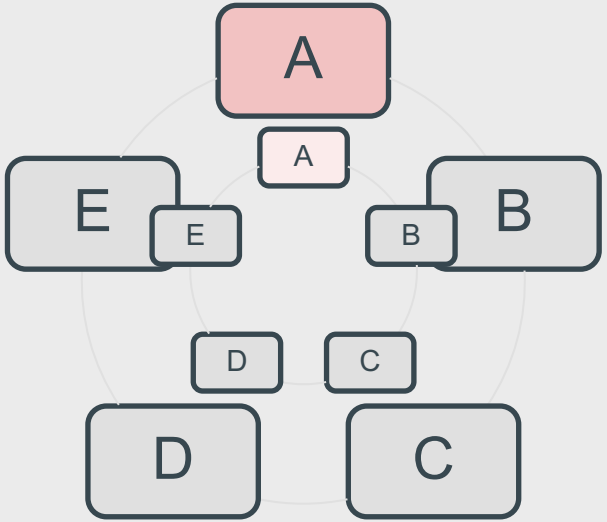


CAESAR CIPHER



KEY IS AMOUNT OF
ROTATION FROM BASE CASE

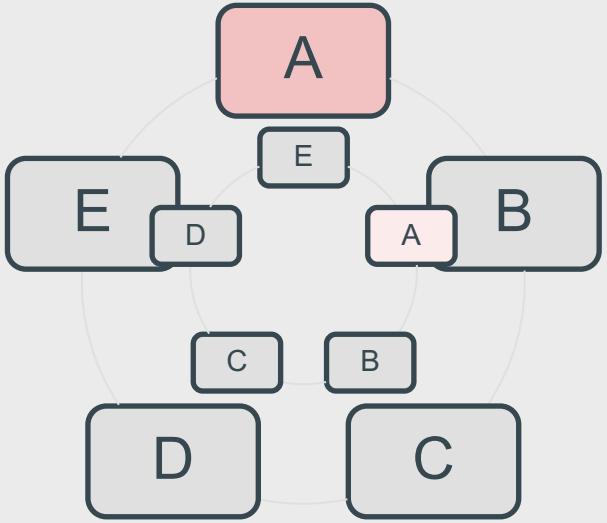
CAESAR CIPHER



Key = 0

Plaintext	A	B	C	D	E
Ciphertext	A	B	C	D	E

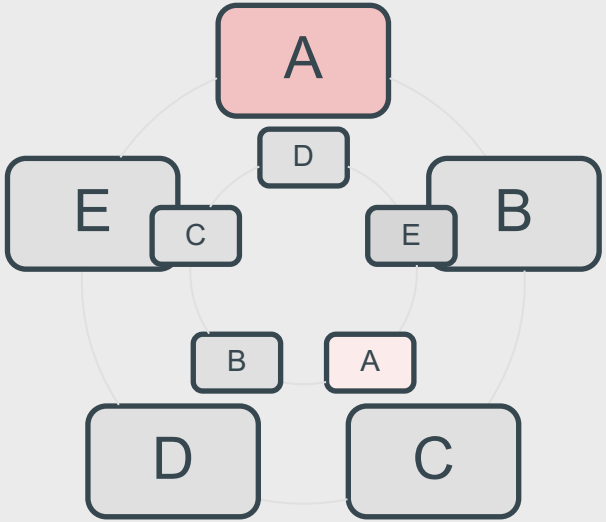
CAESAR CIPHER



Key = 1

Plaintext	A	B	C	D	E
Ciphertext	B	C	D	E	A

CAESAR CIPHER



Key = 2

Plaintext	A	B	C	D	E
Ciphertext	C	D	E	A	B

ENCRYPTION

KEY 3 (A → D)

PLAINTEXT HELLO WORLD

CIPHERTEXT KHOOR ZRUOG

DECRYPTION

KEY 3 (A ← D)

CIPHERTEXT KHOOR ZRUOG

PLAINTEXT HELLO WORLD

ENCRYPTION

Small keyspace

!!

KEY 3 (A → D)

PLAINTEXT HELLO WORLD

CIPHERTEXT KHOOR ZRUOG

!!

Structure maintained

VIGENÈRE CIPHER

WHAT IF THE KEY CHANGED FOR EVERY PLAINTEXT CHARACTER?

VIGENÈRE CIPHER

LETTER	VALUE
A	0
B	1
C	2
D	3
E	4
F	5
G	6
H	7
I	8
J	9
K	10
L	11
M	12

LETTER	VALUE
N	13
O	14
P	15
Q	16
R	17
S	18
T	19
U	20
V	21
W	22
X	23
Y	24
Z	25

WHAT IF THE KEY WAS LETTERS?

VIGENÈRE CIPHER

PASSPHRASE	s	e	c	r	e	t
KEY	18	04	02	17	04	19
PLAINTEXT	a	c	c	e	s	s
CIPHERTEXT	s	g	e	v	w	l

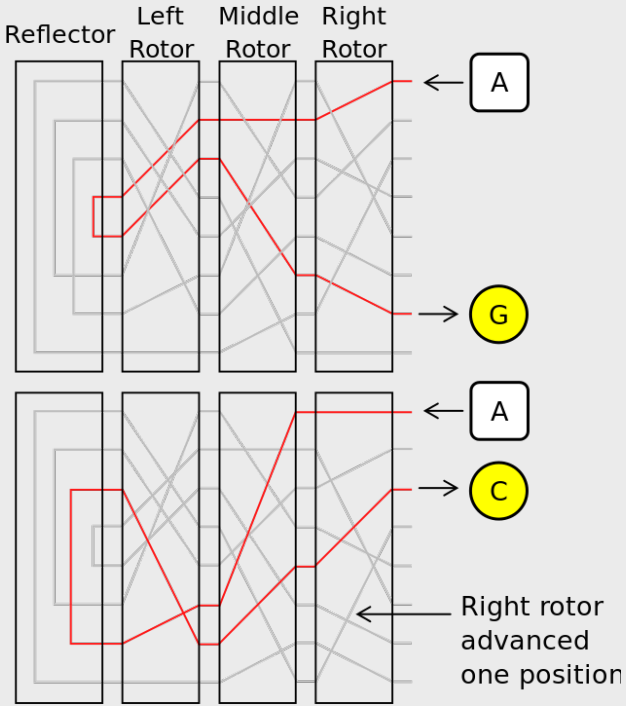
VIGENÈRE CIPHER

WHAT IF THE PLAINTEXT IS LONGER THAN THE KEY?

```
  WHATCOULDPOSSIBLYGOWRONG
+ COMPLETEVICTORYCOMPLETEV
--------------------------
  yvminsnpyxqlgzznmsdhvhrb
```

WHAT IF THE SUBSTITUTION WAS RANDOM-LOOKING AND DIDN'T REPEAT?

ENIGMA



Source: Wikipedia

CODEBOOKS FOR PLAINTEXT LETTERS

FIRST LETTER

Plaintext	Ciphertext
A	N
B	Y
C	F
D	Q
E	B
F	L
G	I
H	W
I	E
J	D
K	M
L	U
M	R

Plaintext	Ciphertext
N	C
O	J
P	T
Q	P
R	S
S	O
T	A
U	K
V	X
W	Z
X	G
Y	V
Z	H

SECOND LETTER

Plaintext	Ciphertext
A	Q
B	F
C	V
D	K
E	R
F	Y
G	L
H	A
I	S
J	Z
K	G
L	B
M	M

Plaintext	Ciphertext
N	H
O	C
P	N
Q	T
R	W
S	O
T	D
U	X
V	I
W	U
X	J
Y	E
Z	P

THIRD LETTER…

Plaintext	Ciphertext
A	I
B	Q
C	A
D	P
E	J
F	U
G	B
H	X
I	K
J	L
K	W
L	C
M	X

Plaintext	Ciphertext
N	R
O	Y
P	D
Q	T
R	V
S	M
T	N
U	E
V	S
W	F
X	O
Y	G
Z	H

CODEBOOKS FOR PLAINTEXT LETTERS

FIRST LETTER

Plaintext	Ciphertext
A	N
B	Y
C	F
D	Q
E	B
F	L
G	I
H	W
I	E
J	D
K	M
L	U
M	R

Plaintext	Ciphertext
N	C
O	J
P	T
Q	P
R	S
S	O
T	A
U	K
V	X
W	Z
X	G
Y	V
Z	H

SECOND LETTER

Plaintext	Ciphertext
A	Q
B	F
C	V
D	K
E	R
F	Y
G	L
H	A
I	S
J	Z
K	G
L	B
M	M

Plaintext	Ciphertext
N	H
O	C
P	N
Q	T
R	W
S	O
T	D
U	X
V	I
W	U
X	J
Y	E
Z	P

THIRD LETTER…

Plaintext	Ciphertext
A	I
B	Q
C	A
D	P
E	J
F	U
G	B
H	X
I	K
J	L
K	W
L	C
M	X

Plaintext	Ciphertext
N	R
O	Y
P	D
Q	T
R	V
S	M
T	N
U	E
V	S
W	F
X	O
Y	G
Z	H

YES → VRM

QUESTIONS?

Contact Prof. Essex:
aessex@uwo.ca
@aleksessex

See course website for slides and videos:
https://whisperlab.org/security