

UNIT 16 *Modern Encryption*

Overhead Slides

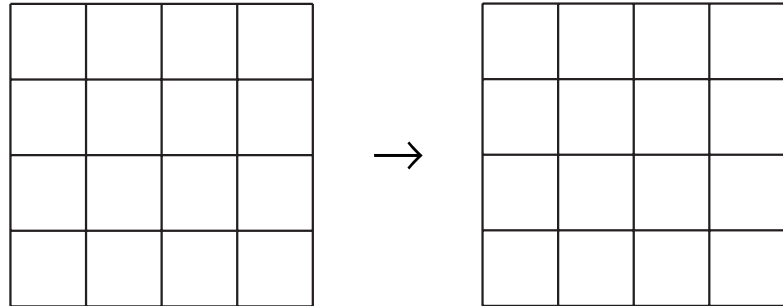
Overhead Slides

- 16.1 Encryption
 - 16.1a Completed Encryption
 - 16.2 Caesar Substitution
 - 16.3 Binary Representation of Letters
 - 16.4 'Addition'
 - 16.5 Decryption
 - 16.5a Completed Decryption
-

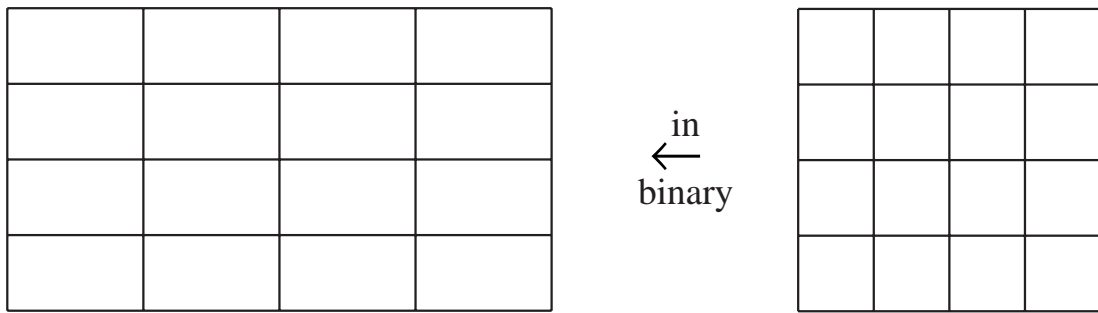
OS 16.1

Encryption

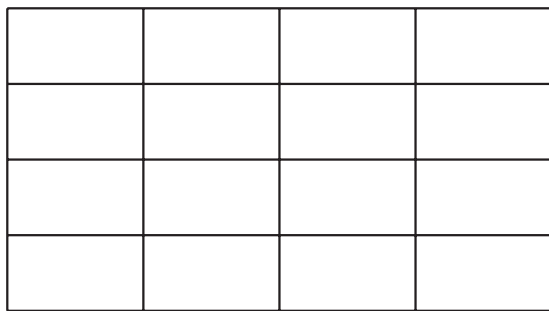
Step 1: Caesar substitution



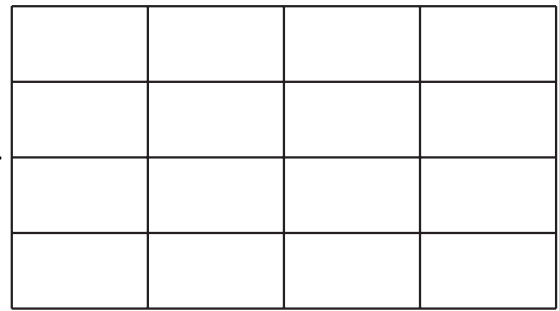
Step 2: row shift



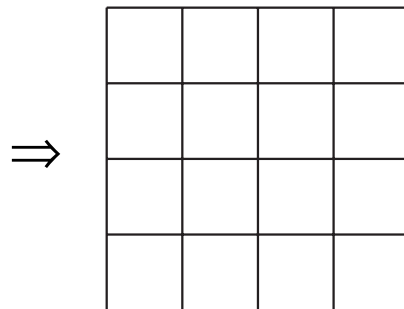
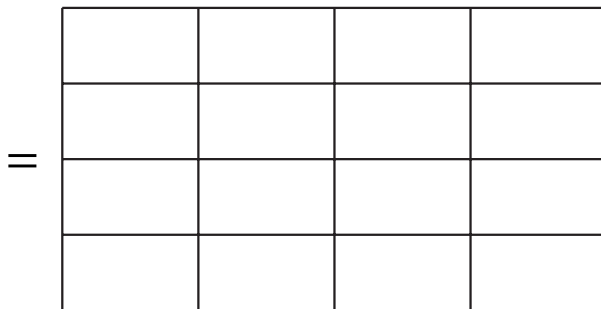
Step 3: column transformation



Step 4: add key



(in binary)



(letters)

Message:

OS 16.1a

Completed Encryption

Step 1: Caesar substitution

M	M	R	N
E	E	E	I
E	H	A	N
T	E	T	E

→

P	P	U	Q
H	H	H	L
H	K	D	Q
W	H	W	H

Step 2: row shift

10000	10000	10101	10001
01000	01000	01100	01000
00100	10001	01000	01011
01000	10111	01000	10111

←

in
binary

P	P	U	Q
H	H	L	H
D	Q	H	K
H	W	H	W

Step 3: column transformation

00100	01110	01100	10100
11100	10110	10101	01101
10000	01111	10001	01110
11100	01001	10001	10010

Step 4: add key

01111	00101	10100	10100
10101	00011	01101	01001
10010	10010	00101	01110
10011	00101	00101	00111

(in binary)

=

01011	01011	11000	00000
01001	10101	11000	00100
00010	11101	10100	00000
01111	01100	10100	10101

⇒

K	K	X	_
I	U	X	D
B	?	T	_
O	L	T	U

(letters)

Message: K I B O K U ? L X X T T _ D _ U

OS 16.2

Caesar Substitution

Plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
Caesar	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
Plaintext	Q	R	S	T	U	V	W	X	Y	Z	,	.	?	'	!	_
Caesar	T	U	V	W	X	Y	Z	,	.	?	'	!	_	A	B	C

OS 16.3

Binary Representation of Letters

Letter	Binary	Letter	Binary	Letter	Binary	Letter	Binary
<space>	00000	H	01000	P	10000	X	11000
A	00001	I	01001	Q	10001	Y	11001
B	00010	J	01010	R	10010	Z	11010
C	00011	K	01011	S	10011	,	11011
D	00100	L	01100	T	10100	.	11100
E	00101	M	01101	U	10101	?	11101
F	00110	N	01110	V	10110	'	11110
G	00111	O	01111	W	10111	!	11111

OS 16.4*'Addition'*

Rules:

$$0 + 0 = 0$$

$$0 + 1 = 1$$

$$1 + 0 = 1$$

$$1 + 1 = 0$$

Example:

$$A + B + C = 00001 + \boxed{} + \boxed{}$$

$$= \boxed{} + \boxed{}$$

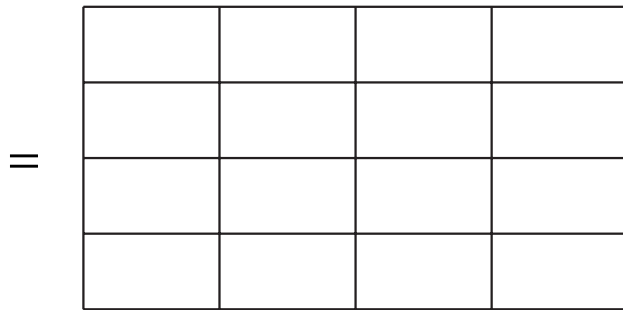
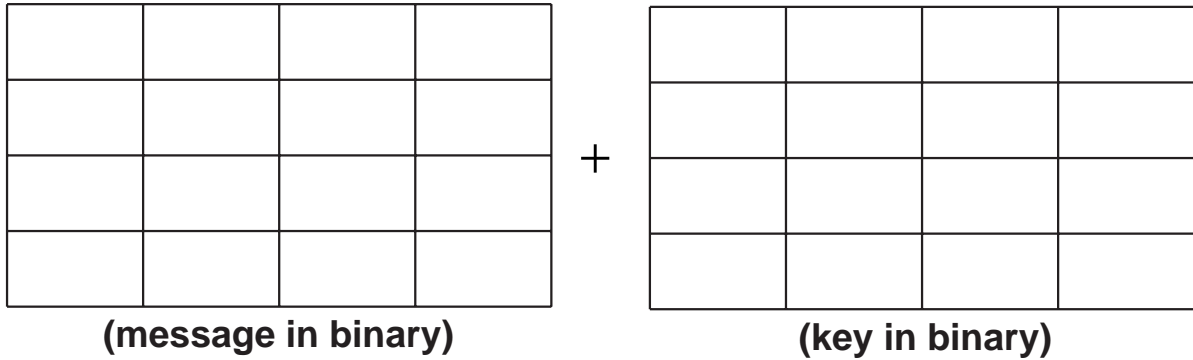
$$= \boxed{}$$

$$= \boxed{}$$

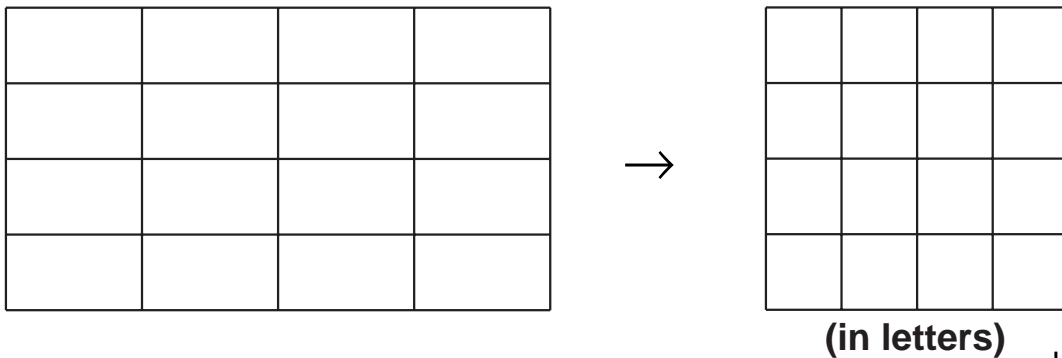
OS 16.5

Decryption

Step 1: add key

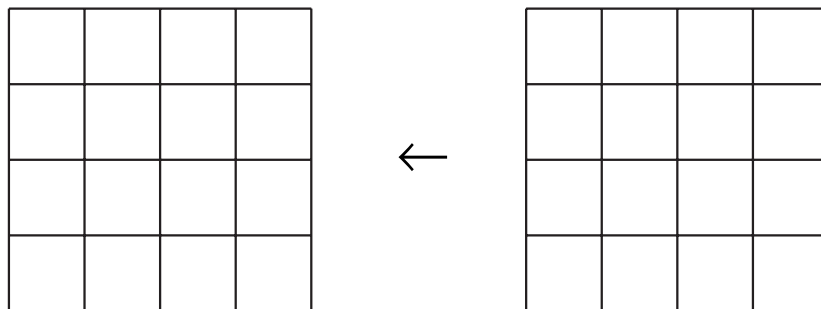


Step 2: column transformations



Step 4: substitution

Step 3: row shift



Message:

OS 16.5a

Completed Decryption

Step 1: add key

01011	01011	11000	00000
01001	10101	11000	00100
00010	11101	10100	00000
01111	01100	10100	10101

+

01111	00101	10100	10100
10101	00011	01101	01001
10010	10010	00101	01110
10011	00101	00101	00111

(message in binary) (key in binary)

=

00100	01110	01100	10100
11100	10110	10101	01101
10000	01111	10001	01110
11100	01001	10001	10010



Step 2: column transformations

10000	10000	10101	10001
01000	01000	01100	01000
00100	10001	01000	01011
01000	10111	01000	10111

→

P	P	U	Q
H	H	L	H
D	Q	H	K
H	W	H	W

(in letters)



Step 4: substitution

Step 3: row shift

M	M	R	N
E	E	E	I
E	H	A	N
T	E	T	E

←

P	P	U	Q
H	H	H	L
H	K	D	Q
W	H	W	H

Message: MEET ME HERE AT NINE