Cryptography
ECE5632 - Spring 2025

Lecture 2B

Dr. Farah Raad

Lecture Topic

Stream Ciphers

Concepts from Linear Algebra

- To explain how the inverse of a matrix is computed, we begin by with the concept of **determinant**.
- For any square matrix **($m \times m$),** the **determinant** equals the sum of all the products that can be formed by taking exactly one element from each row and exactly one element from each column, with certain of the product terms preceded by a minus sign.
- **For a (2×2) matrix**

$$\begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix}$$

the determinant is $k_{11}k_{22} - k_{12}k_{21}$.

- **For (3×3) matrix, the value of the determinant is**

$$k_{11}k_{22}k_{33} + k_{21}k_{32}k_{13} + k_{31}k_{12}k_{23} - k_{31}k_{22}k_{13} - k_{21}k_{12}k_{33} - k_{11}k_{32}k_{23}.$$

Concepts from Linear Algebra

➢ If a square matrix **A** has a nonzero determinant, then the inverse of the matrix is computed as

$$[A^{-1}]_{ij} = (\det A)^{-1}(-1)^{i+j}(D_{ji})$$

- (D_{ji}) is the subdeterminant formed by deleting the j row and the i column of **A**,
- det(**A**) is the determinant of **A**,
- $(det\ A)^{-1}$ is the multiplicative inverse of (det **A**) mod 26.

Continuing our example

$$\det\begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix} = (5 \times 3) - (8 \times 17) = -121 \bmod 26 = 9$$

We can show that $9^{-1} \bmod 26 = 3$, because $9 \times 3 = 27 \bmod 26 = 1$

$$\mathbf{A} = \begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix}$$

$$\mathbf{A}^{-1} \bmod 26 = 3\begin{pmatrix} 3 & -8 \\ -17 & 5 \end{pmatrix} = 3\begin{pmatrix} 3 & 18 \\ 9 & 5 \end{pmatrix} = \begin{pmatrix} 9 & 54 \\ 27 & 15 \end{pmatrix} = \begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix}$$

Concepts from Linear Algebra

- We define the inverse $\mathbf{M}^{-1}$ of a square matrix $\mathbf{M}$ by the equation, where $\mathbf{I}$ is the identity matrix.
- $\mathbf{I}$ is a square matrix that is all zeros except for ones along the main diagonal from upper left to lower right.
- The inverse of a matrix does not always exist, but when it does, it satisfies the preceding equation.

$$\mathbf{A} = \begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix} \qquad \mathbf{A}^{-1} \bmod 26 = \begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix}$$

$$\begin{aligned} \mathbf{AA}^{-1} &= \begin{pmatrix} (5 \times 9) + (8 \times 1) & (5 \times 2) + (8 \times 15) \\ (17 \times 9) + (3 \times 1) & (17 \times 2) + (3 \times 15) \end{pmatrix} \\ &= \begin{pmatrix} 53 & 130 \\ 156 & 79 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

Monoalphabetic Ciphers

- Monoalphabetic ciphers: A single mapping is used per a message alphabet.
  e.g., Caesar, Affine, etc.
- **Problem:** Frequency data of the original alphabet is preserved.
- **Two approaches to lessen this problem:**
  - Encrypt multiple letters of plaintext. i.e., Multi-letter ciphers.
  - Use multiple cipher alphabets. i.e., Polyalphabetic ciphers

Hill Cipher (a multi-letter cipher)

- Encrypts m plaintext letters at a time.

$$Y = X.K \bmod 26$$

$$X = Y.K^{-1} \bmod 26 = X.K.K^{-1} \bmod 26 = X$$

This can be expressed in terms of row vectors and matrices:

e.g., m=2: $$(y_1 \quad y_2) = (x_1 \quad x_2)\begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix} \bmod 26$$

Hill Cipher (a multi-letter cipher)

➢ Hill Cipher: Encryption Example

Encrypt x = cat, using the following Hill cipher key:

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Then $Y = (y_1 \quad y_2 \quad y_3) = (2 \quad 0 \quad 19)\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$

Then $Y = (72 \quad 72 \quad 371) \bmod 26$

$= (20 \quad 20 \quad 7) \bmod 26$

$= uuh$

Hill Cipher (a multi-letter cipher)

➢Hill Cipher: Decryption Example

Now decrypt y = uuh, using the same Key

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \xrightarrow{\text{Linear Algebra}} K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

Then $X = (x_1 \quad x_2 \quad x_3) = (20 \quad 20 \quad 7) \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \text{mod} 26$

Then $X = (548 \quad 520 \quad 539) \bmod 26$

$= (2 \quad 0 \quad 19) \bmod 26$

= cat

Hill Cipher (a multi-letter cipher)

➢ Hill Cipher: Encryption Example

Consider the plaintext "paymoremoney" and use the encryption key

$$\mathbf{K} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Hill Cipher (a multi-letter cipher)

➢ Hill Cipher: Encryption Example

Consider the plaintext "paymoremoney" and use the encryption key

$$\mathbf{K} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

The ciphertext is RRLMWBKASPDH

Hill Cipher

- Larger m, hides more frequency information.
- Strong against ciphertext-only attacks.
- Easy to break by known-plaintext attacks.

Hill Cipher: Known-plaintext Attack

Assuming m plaintext-ciphertext (X_j-Y_j) pairs;

$$X_j(x_{j1} \quad x_{j2} \quad \cdots \quad x_{jm}) \rightarrow Y_j(y_{j1} \quad y_{j2} \quad \cdots \quad y_{jm})$$

Such that $Y_j = X_j.K$ for $1 \leq j \leq m$

construct an m x m matrix $P = \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_m \end{pmatrix}$ and $C = \begin{pmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_m \end{pmatrix}$

Therefore, $K = P^{-1}C$

If P is not invertible, requires additional X-Y pairs.

Hill Cipher: Known-plaintext Attack

- Hill Cipher: Attack Example

Suppose that the plaintext "hillcipher" is encrypted using a 2×2 Hill cipher to yield the ciphertext "HCRZSSXNSP".

x= hillcipher , m=2 , y=HCRZSSXNSP, get K

Known: (7 8)K mod 26 = (7 2);

(11 11)K mod 26= (17 25)

and so on. Using the first two plaintext–ciphertext pairs

$$\text{So, } C = PK \bmod 26 = \begin{pmatrix} 7 & 2 \\ 17 & 25 \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} K \bmod 26$$

$$P^{-1} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}^{-1} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \bmod 26$$

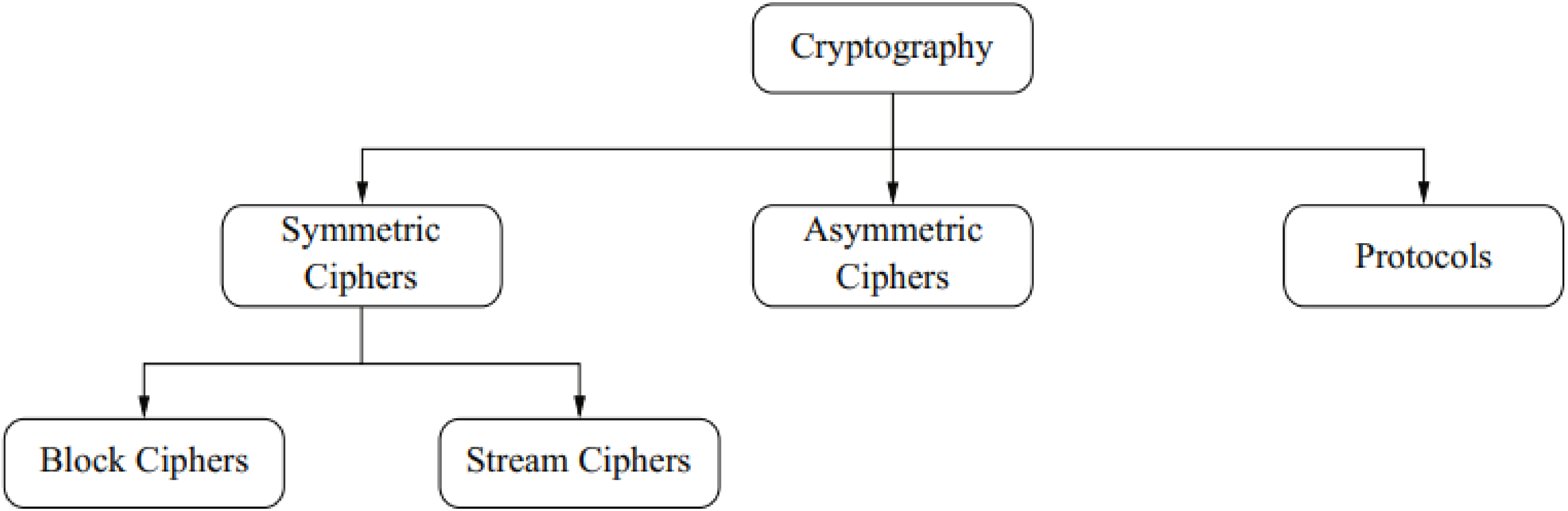
$$K = P^{-1}C = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} 7 & 2 \\ 17 & 25 \end{pmatrix} = \begin{pmatrix} 549 & 600 \\ 398 & 577 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 3 & 2 \\ 8 & 5 \end{pmatrix}$$

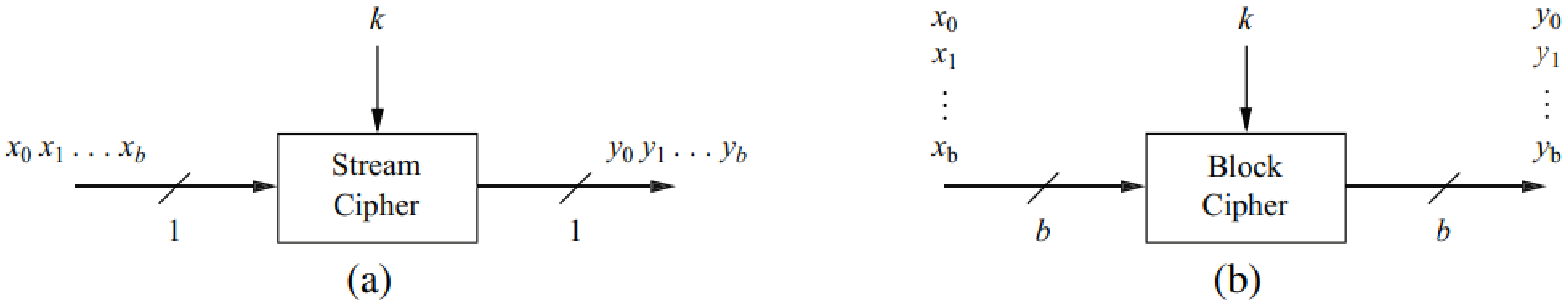
Check: Test with remaining known X_j-Y_j pairs.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Main Areas of Cryptography



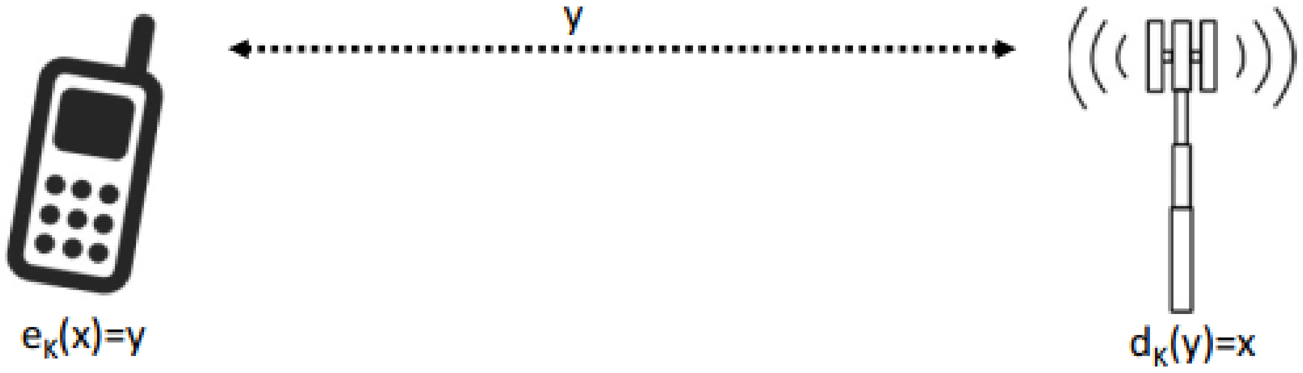
Stream Ciphers vs Block Ciphers



- **Stream Ciphers**
  - Encrypt bits individually
  - Usually small and fast → common in embedded devices (e.g., A5/1 for GSM phones)
- **Block Ciphers:**
  - Always encrypt a full block (several bits)
  - Are common for Internet applications

Stream Ciphers

- Example of a popular application: **GSM cell phone**



Stream Ciphers

- A stream cipher encrypts bits individually:
- Plaintext x_i, ciphertext y_i and key stream S_i consist of individual bits

plaintext ciphertext key stream

$$\text{for } x_i, y_i, s_i \in \{0,1\} \text{ (i.e., } \in Z_2)$$

- Encryption and decryption are simple additions modulo 2 (aka XOR)
- Encryption and decryption are the same functions

$$\text{Encryption: } y_i = e_{s_i}(x_i) \equiv x_i + s_i \bmod 2.$$

$$\text{Decryption: } x_i = d_{s_i}(y_i) \equiv y_i + s_i \bmod 2.$$

Stream Ciphers

- Proof: Decryption function same as encryption.

$$\begin{aligned} d_{s_i}(y_i) &\equiv y_i + s_i \bmod 2 \\ &\equiv (x_i + s_i) + s_i \bmod 2 \\ &\equiv x_i + 2s_i \bmod 2 \\ &\equiv x_i + 0 \bmod 2 \\ &\equiv x_i \bmod 2 \end{aligned}$$

- Note: mod 2 addition and subtraction are the same operation.

Stream Ciphers

Modular 2 Addition

- The truth table of mod 2 addition:

x_i	s_i	$y_i \equiv x_i + s_i \bmod 2$
0	0	0
0	1	1
1	0	1
1	1	0

  - i.e., the same truth table of an XOR gate.

Stream Ciphers

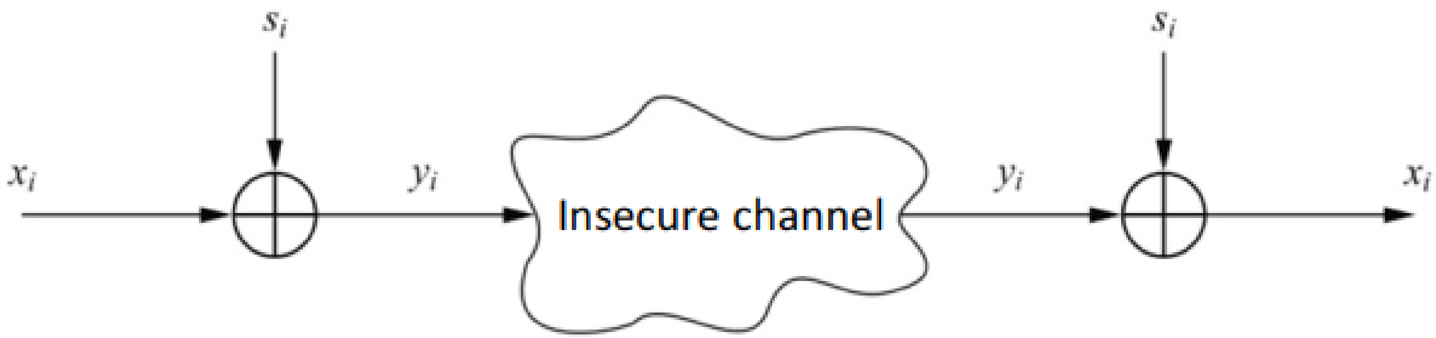
Modular 2 Addition

- **Why is Modulo 2 Addition a Good Encryption Function?**

  - Modulo 2 addition is equivalent to XOR operation
  - For perfectly random key stream s_i, each ciphertext output bit has a 50% chance to be 0 or 1
  - Good statistic property for ciphertext
  - Inverting XOR is simple, since it is the same XOR operation

Stream Ciphers

- General communication model



Stream Ciphers

➢ **Example :** **Encrypt the letter A. (assume key stream bits: 0101100)**

$x_7 \ldots x_1 = 1000001_2$ ASCII value for A

$s_7 \ldots s_1 = 0101100$

$y_7 \ldots y_1 = 1101101 \xrightarrow{\text{ASCII value for } \mathbf{m}}$

$1101101 = y_i$

$0101100 = s_i$

$1000001 = x_i$

"A"

MSA UNIVERSITY
IN EGYPT SINCE 1996
Established by Dr.Nawal El Degwi
MSA UNIVERSITY
جامعة أكتوبر للعلوم الحديثة والآداب

Thank You!

See You next Lectures!!

Any Question?

26th July Mehwar Road Intersection with Wahat Road, 6th of October City, Egypt
Tel: +202383711146 Fax: +20238371543 Postal code: 12451
Email: info@msa.eun.eg Hotline: 16672 Website: www.msa.edu.eg