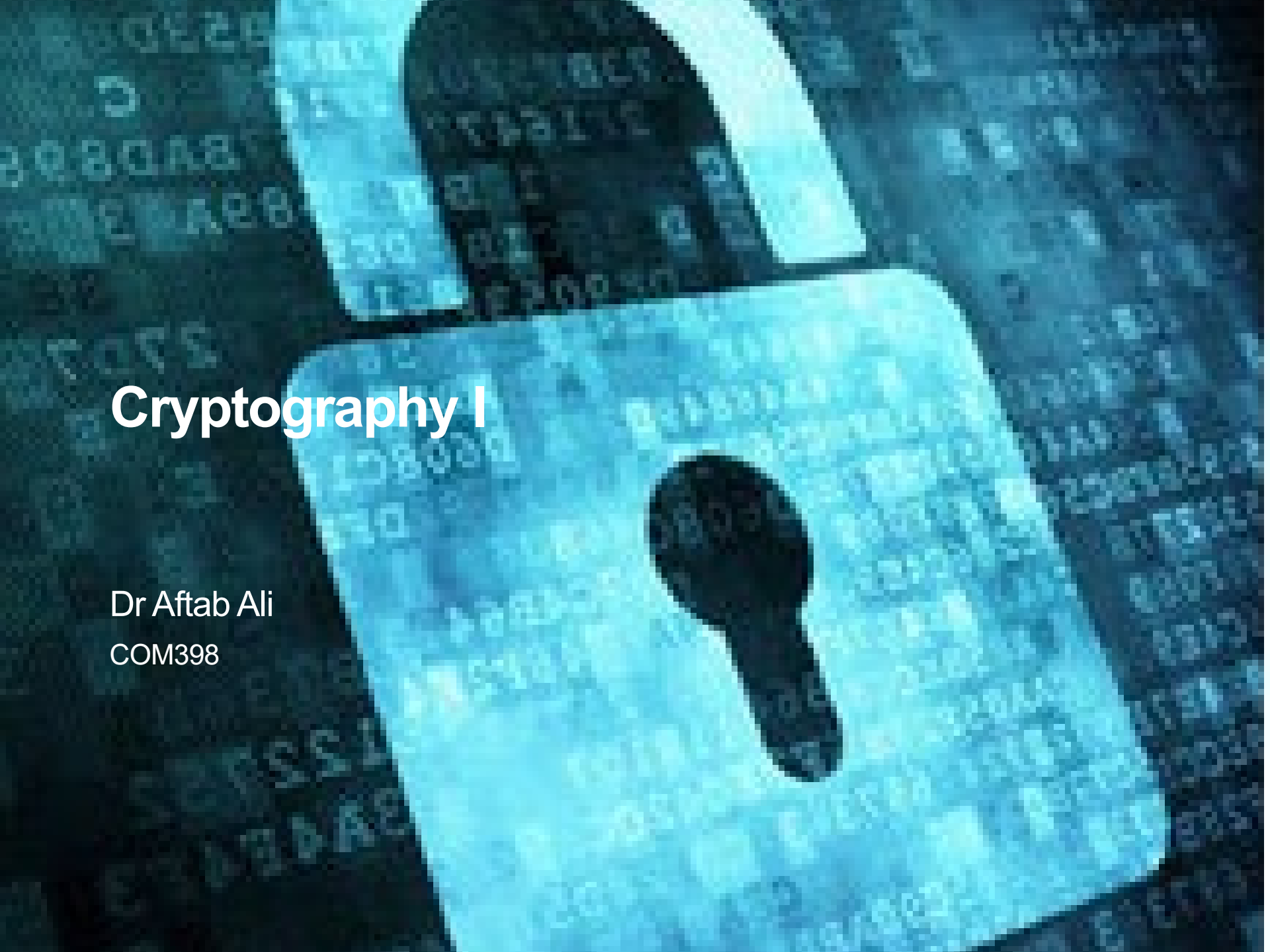


Cryptography I

Dr Aftab Ali

COM398

Introduction

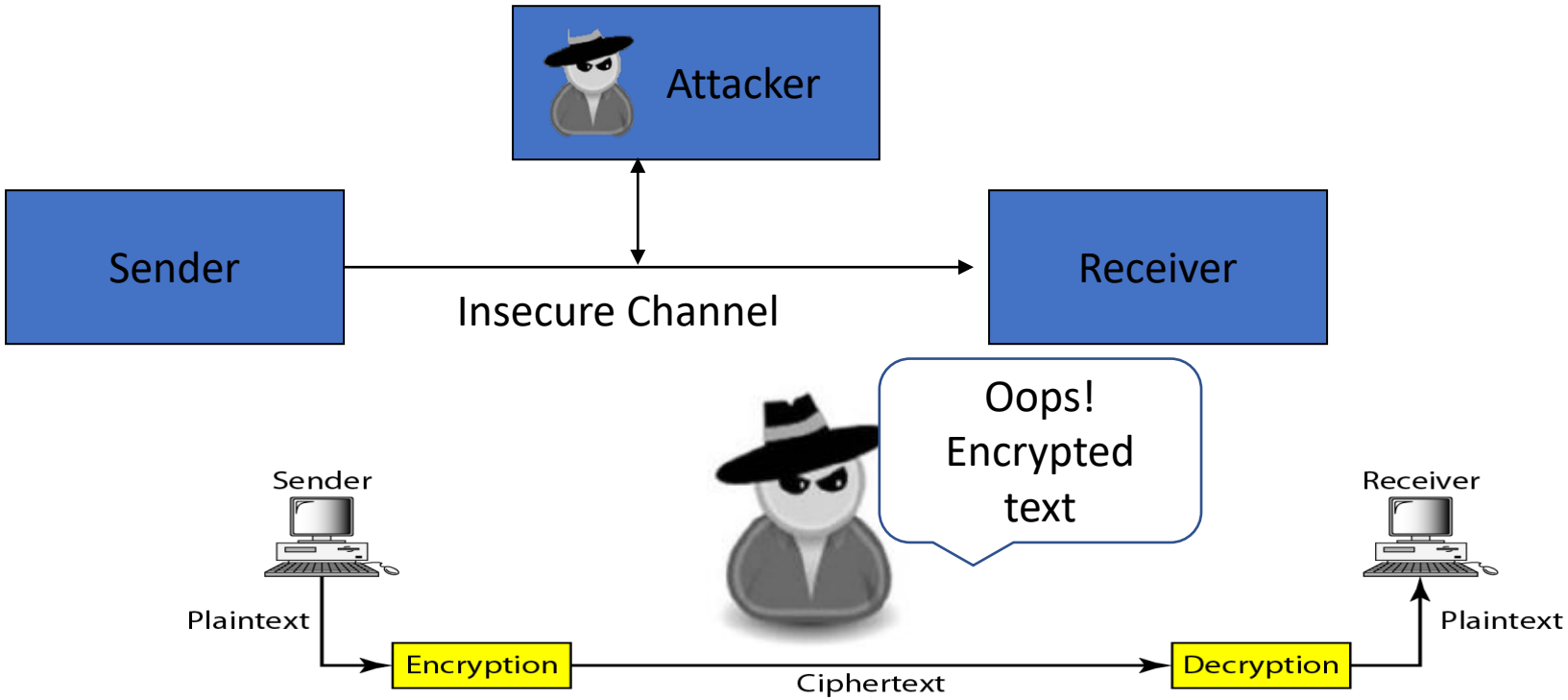
- Cryptography: Definition
- Data Security
- Historical Background
  - Caesar cipher
  - Vigenere Cipher
- Symmetric Encryption
  - One time pad
  - ROT13
  - Stream ciphers
  - Block ciphers

Cryptography

What is cryptography

- **Cryptography**
  - The art of secret writing
  - Cryptography is the making
- **Cryptanalysis**
  - Cryptanalysis is the breaking

- **Why Cryptography**
  - Cryptography aims to provide secure communications in the presence of an adversary/attacker.



Cryptography

Some definitions

• **Plaintext:** This is the original message or data that is to be secured.

• **Encryption algorithm: This is the mechanism of securing the message and data.** The encryption algorithm performs various substitutions and transformations on the plaintext.

• **Secret key**: The secret key is also input to the algorithm. The exact substitutions and transformations performed by the algorithm depend on the key.

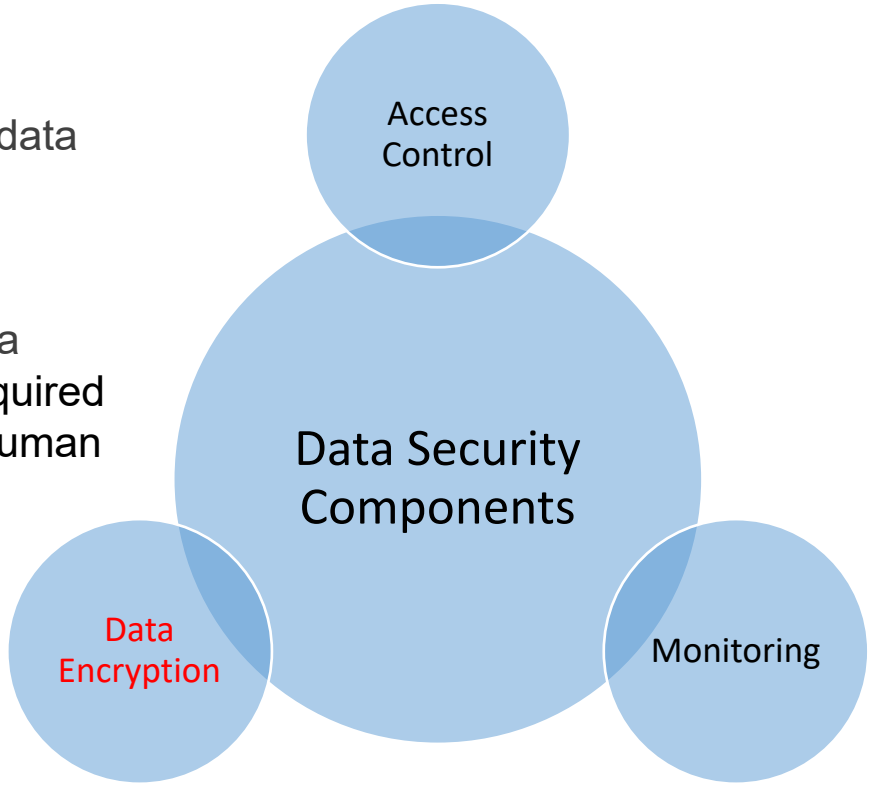
• **Ciphertext**: This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts.

• **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the same secret key and produces the original plaintext.

Data Security

Data Security Components

- **Encrypting data at rest** protects the data where it's stored (on a computer, phone, database)
- **Encrypting data in transit** protects the data as it communicates from one location to another (sending an email, browsing the Internet)
- **Access control** who can access the data
- **Data encryption** strong encryption is required to transform the data from plaintext (or human readable format) to cipher text



Historical Background

The Caesar cipher

- **Caesars cipher**
  - Replace every ‘A’ in the message with a ‘D’
  - Replace every ‘B’ in the message with a ‘E’
  - Replace every ‘C’ in the message with a ‘F’, etc.

- **Considerations**
  - Algorithms are public (Kerchoff’s Principle)
  - Encrypt/decrypt depends on a key
  - The only secret is the key
  - For Caesars cipher, key is ***n***, since shift forward ***n*** to encrypt, shift backward n to decrypt
  - Encryption: $C_i = (P_i + n) \bmod 26$
  - Decryption: $P_i = (C_i - n) \bmod 26$

Historical Background

Cryptanalysis of Caesar Cipher

- **Ciphertext = "GRR MGAR OY JOBOJKJ OT ZNXKK VGXZY"**
- **Perform decryption with each possible key:**
- **Plaintext with n= 1**

  FQQ LFZQ NX INANIJI NS YMWJJ UFWYX
- **Plaintext with n= 2**

  EPP KEYP MW HMZMHIH MR XLVII TEVXW
- **Plaintext with n= 3**

  DOO JDXO LV GLYLGHG LQ WKUHH SDUWV
- **Plaintext with n= 4**

  CNN ICWN KU FKXKFGF KP VJTGG RCTVU
- **Plaintext with n= 5**

  BMM HBVM JT EJWJEFE JO UISFF QBSUT
- **Plaintext with n= 6**

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

Ulster University

Historical Background

Cryptanalysis of Caesar Cipher

- **Ciphertext = "GRR MGAR OY JOBOJKJ OT ZNXKK VGXZY"**
- **Perform decryption with each possible key:**
- **Plaintext with n= 1**

  FQQ LFZQ NX INANIJI NS YMWJJ UFWYX
- **Plaintext with n= 2**

  EPP KEYP MW HMZMHIH MR XLVII TEVXW
- **Plaintext with n= 3**

  DOO JDXO LV GLYLGHG LQ WKUHH SDUWV
- **Plaintext with n= 4**

  CNN ICWN KU FKXKFGF KP VJTGG RCTVU
- **Plaintext with n= 5**

  BMM HBVM JT EJWJEFE JO UISFF QBSUT
- **Plaintext with n= 6**

  ALL GAUL IS DIVIDED IN THREE PARTS

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

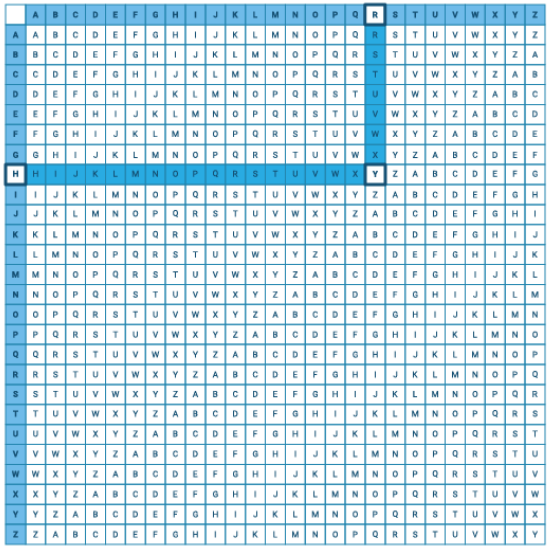
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
13	14	15	16	17	18	19	20	21	22	23	24	25

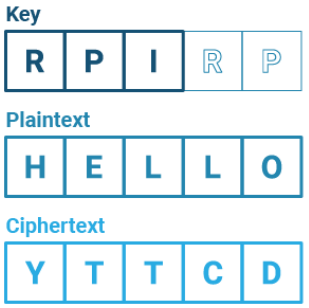
Ulster University

Historical Background

Vigenere Cipher

- Developed in 1553.
- It is a method of encrypting alphabetic text by using a series of interwoven Caesar ciphers, based on the letters of a keyword.





- **Key**: A word W of Length M.
- **Plain text** P of length N.
- Repeat the Key until it matches the length of the plain text.
- For each letter P_j of the plain text, apply a Caesar Cipher of length W_j

- **Example**
- Key: **RPI**
- Plain Text: HELLO
- Expanded key: RPIRP
- Cipher Text: YTTCD

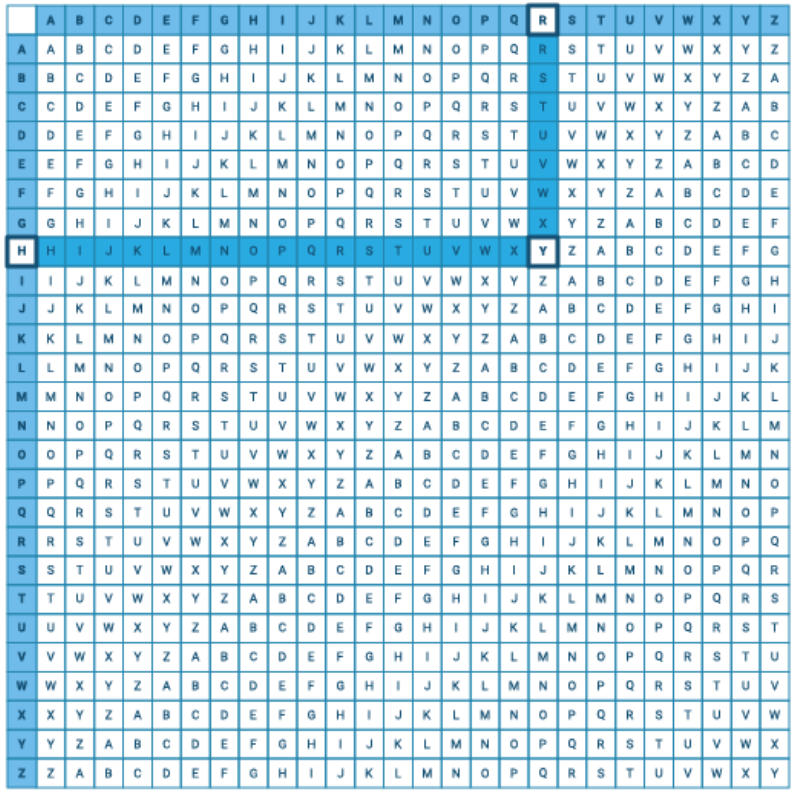
Historical Background

Cryptanalysis of Vigenere Cipher

- Find the length of the key.
  - Kasisky test
- Divide the message into that many shift cipher encryptions.
- Use frequency analysis to solve the resulting shift ciphers.
  - How?
- Key
  - KINGKINGKINGKINGKINGKING
- PlainText
  - The sun and the man in the moon
- Cipher Text
  - D P R Y E V N T N **B U K** W I A O X **B U K** W W B T

Exercise

- ***The apple is in the corner and the pear is there too (plain)***
- ***cat (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	Y	Z
A	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	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	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	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	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	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	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	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
I	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	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	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
N	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
O	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	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

Answer

- ***Vhx cpine bu ig vhx eokpek cnw vhx rett il vhxte mqo (cipher)***

Hill Cipher

- Developed by the mathematician Lester Hill in 1929
- Strength is that it completely hides single-letter frequencies
  - The use of a larger matrix hides more frequency information
  - A 3 x 3 Hill cipher hides not only single-letter but also two-letter frequency information
- Strong against a ciphertext-only attack but easily broken with a known plaintext attack

Ulster University

Hill Cipher

- Plaintext: ACT
- Key: GYBNQKURP
- Ciphertext: POH
- We have to encrypt the message ‘ACT’ (n=3).The key is ‘GYBNQKURP’ which can be written as the nxn matrix:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

Ulster University

Hill Cipher

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \pmod{26}$$

P=15, O=14, H=7 => POH

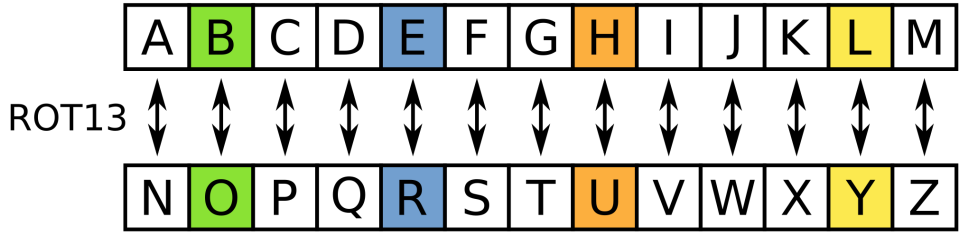
A	B	C	D	E	F	G	H	I	J	K	L	M
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
0	1	2	3	4	5	6	7	8	9	10	11	12

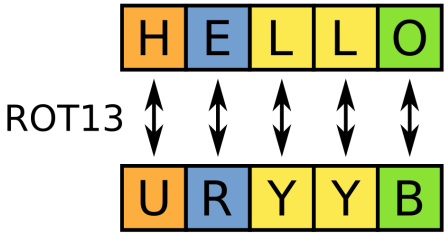
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
13	14	15	16	17	18	19	20	21	22	23	24	25

Ulster University

ROT13

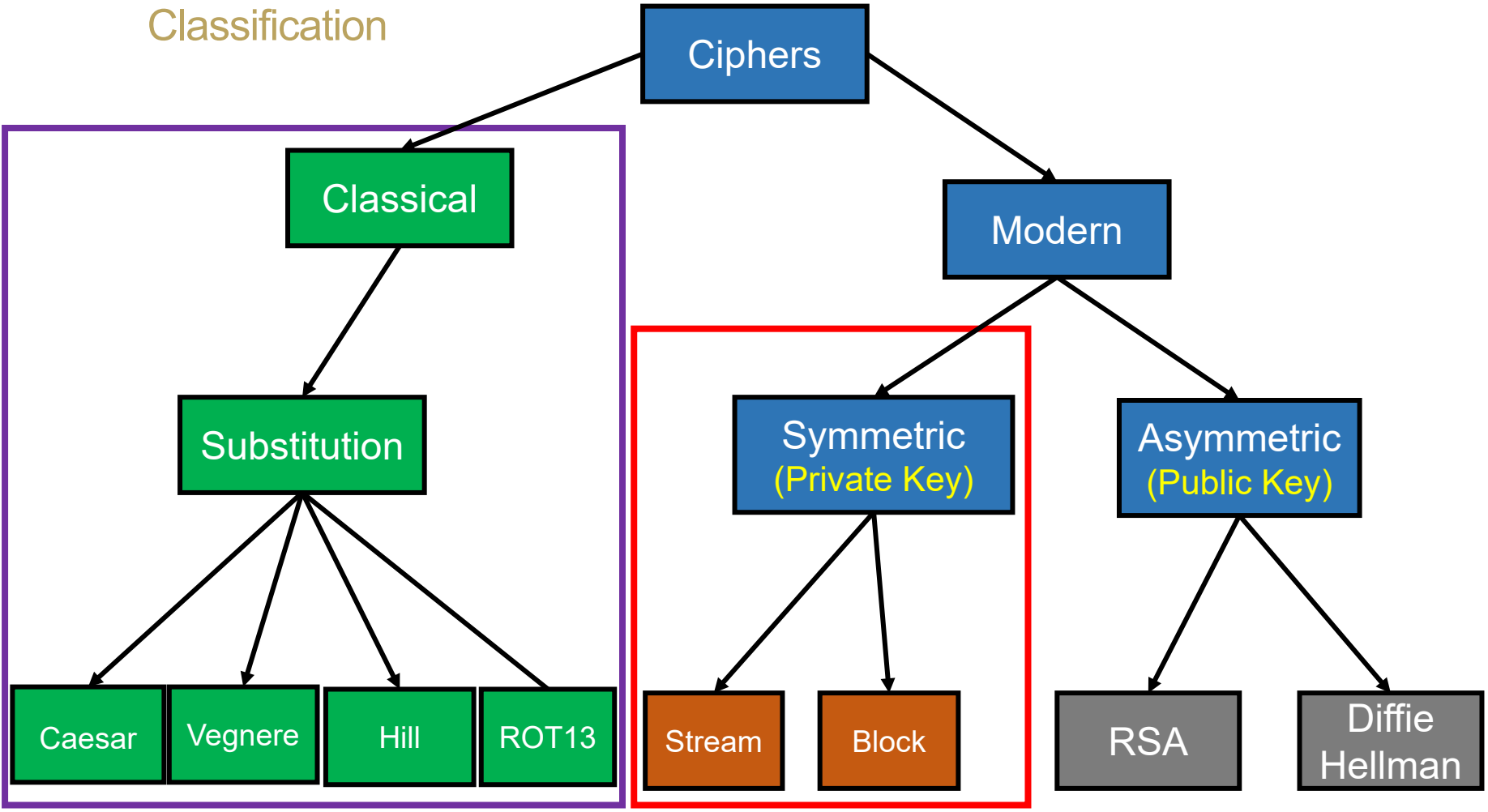
- Poor Encryption: ROT13
  - No “key”
  - Susceptible to frequency analysis
  - Susceptible to brute forcing





What we have covered

Classification



Modern Cryptography

Modern Cryptography may be divided in the following areas:

- Symmetric Cryptography
  - One Key or private key
- Public Key or Asymmetric Cryptography
  - Public Key
  - Private Key
- Cryptanalysis
  - Find any weakness or insecurity in a cryptographic scheme

Symmetric Encryption

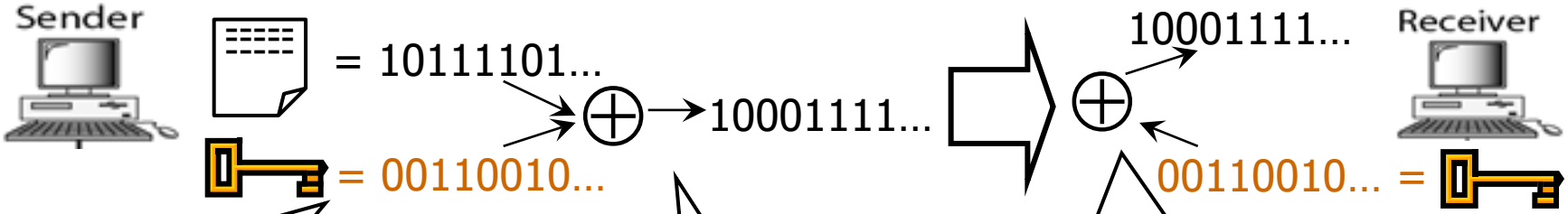
- The universal technique for providing confidentiality for transmitted or stored data
- Also referred to as conventional encryption or single-key encryption

- Two requirements for secure use:
  - Need a strong encryption algorithm*
  - Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure

One Time Pad

A first example of Symmetric Encrpytion

- Invented by Gilbert Vernam in the 1920s
- The message is a bitstring $m \epsilon \{0,1\}^n$
- The key is a bitstring as long as the message, $k \epsilon \{0,1\}^n$
- Encryption is similar to shift cipher
- The ciphertext is obtained by XORing each bit of the plaintext with each bit of the key: c = m ⊕ k.



Key is a random bit sequence as long as the plaintext

Encrypt by bitwise XOR of plaintext and key:
ciphertext = plaintext ⊕ key

Decrypt by bitwise XOR of ciphertext and key:
ciphertext ⊕ key =
(plaintext ⊕ key) ⊕ key =
plaintext ⊕ (key ⊕ key) =
plaintext

One Time Pad

Advantages

- **Easy to compute**
  - Encryption and decryption are the same operation
  - Bitwise XOR is very cheap to compute
- **As secure as theoretically possible**
  - Given a ciphertext, all plaintexts are equally likely, regardless of attacker's computational resources
  - if and only if the key sequence is truly random
    - —True randomness is expensive to obtain in large quantities

One Time Pad

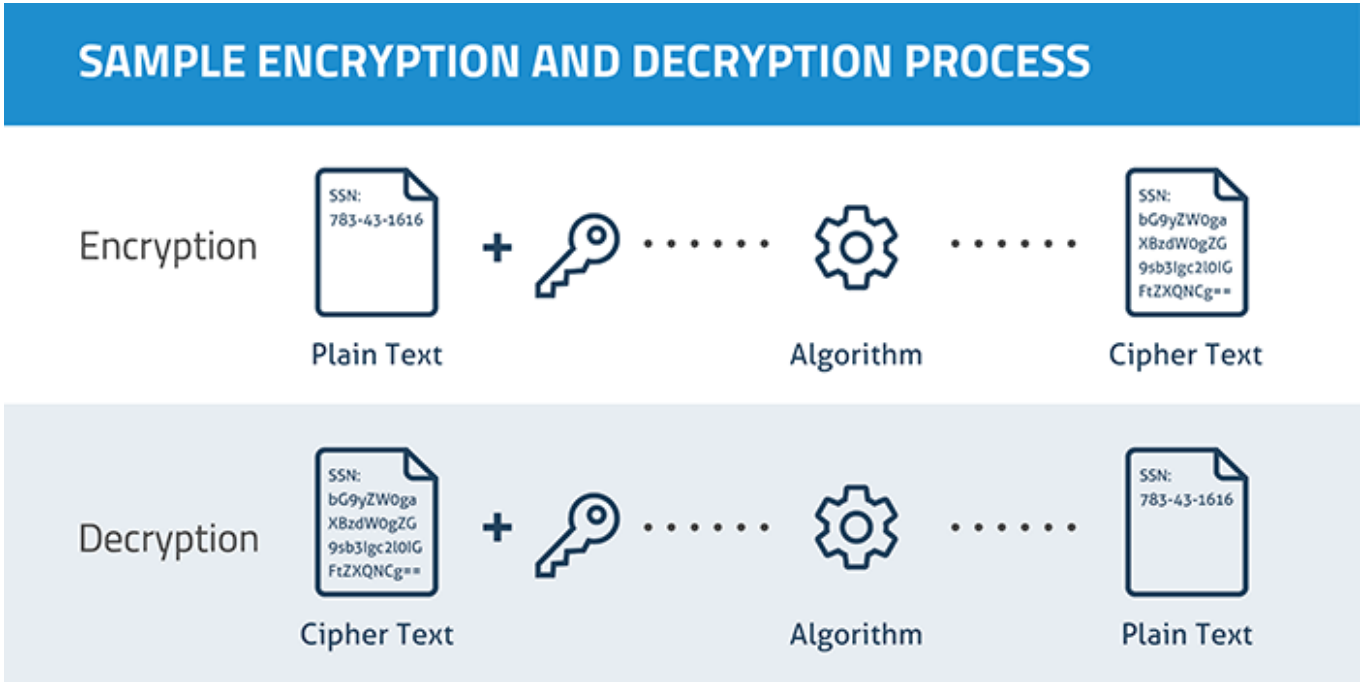
Disadvantages

- **Key must be as long as the plaintext**
  - Impractical in most realistic scenarios
  - Still used for diplomatic and intelligence traffic
- **Does not guarantee integrity**
  - One-time pad only guarantees confidentiality
  - Attacker cannot recover plaintext, but can easily change it to something else
- **Insecure if keys are reused**
  - Attacker can obtain XOR of plaintexts

Symmetric Encryption

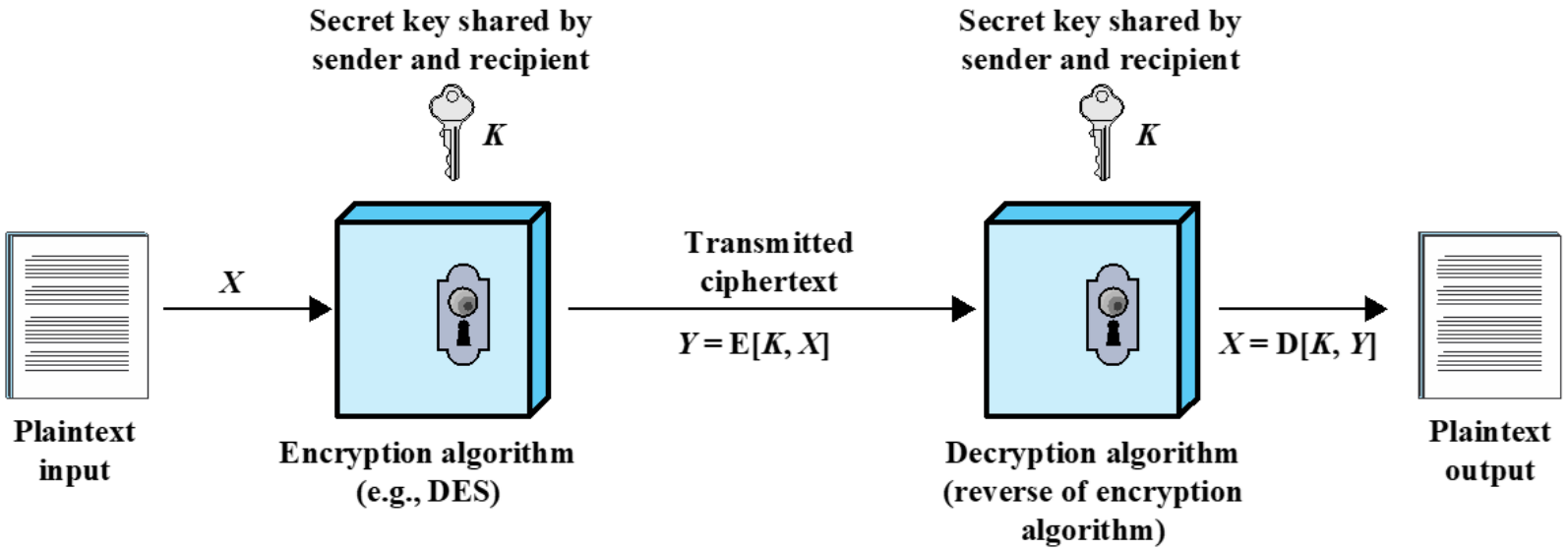
Operational Overview

- Securing data using a key



Symmetric Encryption

Operational Overview



Symmetric Encryption

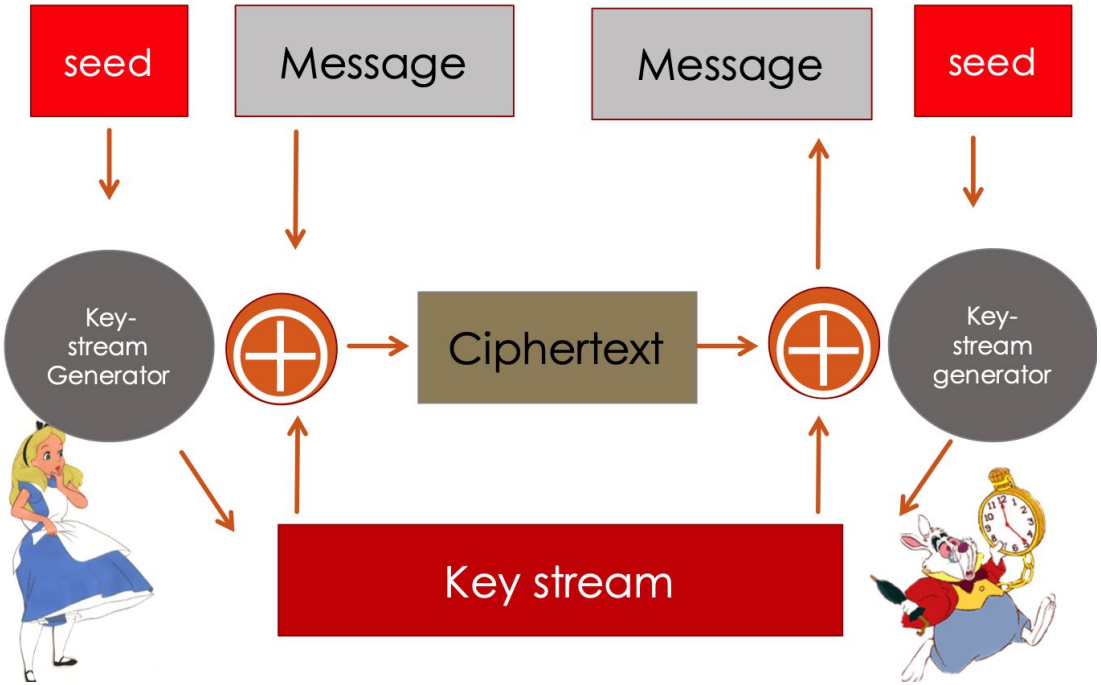
Operational Modes

Symmetric encryption schemes follows two distinct modes of operation:

- **Stream Cipher**
  - Plain text is encrypted bit by bit
  - Plain text and key are XORed
- **Block Cipher**
  - Plain text is encrypted block by block
  - The whole block is encrypted with a key

Stream Ciphers

- Each bit of plaintext is encrypted one by one, with the corresponding bit of the keystream, obtaining a bit of ciphertext.
- To describe a stream cipher, it is enough to describe the key stream generator. Once the key stream is obtained, it works like the one- time pad.
- The key stream must be generated from a random seed



Symmetric Encryption

Stream Encryption

XOR GATE Truth Table

INPUT		OUTPUT
A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

BOOLEAN EXPRESSION

$$A \cdot \overline{B} + \overline{A} \cdot B$$

$$(A + B) \cdot (\overline{A} + \overline{B})$$

$C = A \oplus B$

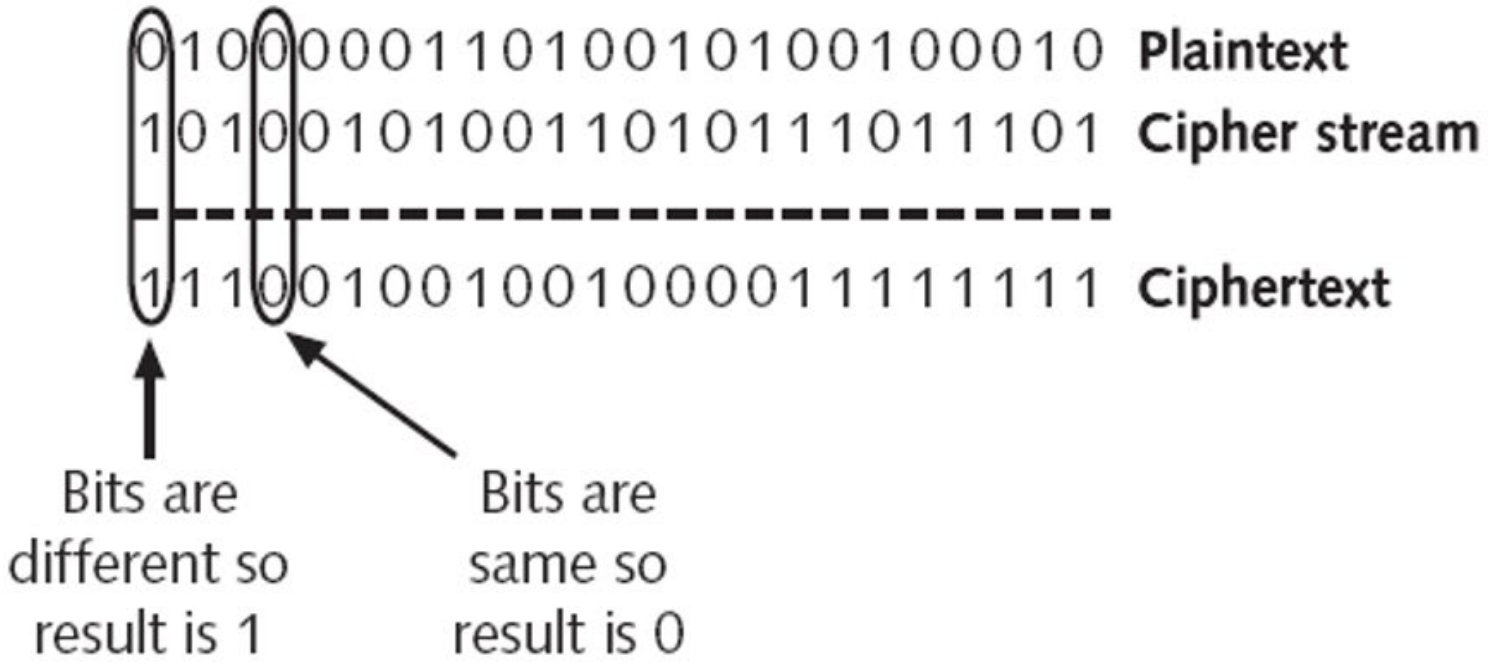
Input1

Input2

Output

Symmetric Encryption

Operational Modes – Stream Encryption



Block Ciphers

- Block ciphers operate on blocks of plaintext one at a time to produce blocks of ciphertext.
- The encryption of a bit in a plaintext will depend on the other bits in the block.
- The block sizes are usually reasonably large. For example, blocks in DES are of 64 bits and block in AES are 128 bits.
- The most famous block cipher is DES (Data Encryption Standard).
- Since DES is the most studied scheme and the design principles DES is based on have inspired a lot of ciphers used nowadays, we will have a slight view of DES.

Symmetric Encryption

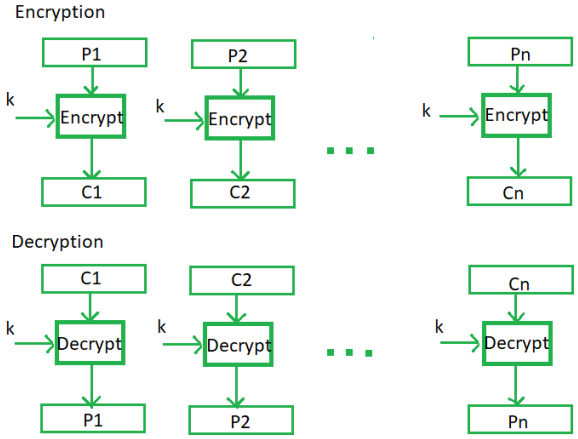
Block Cipher Modes

Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of 64 plaintext bits is encoded independently using the same key.	•Secure transmission of single values (e.g., an encryption key)
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of ciphertext.	•General-purpose block-oriented transmission •Authentication
Cipher Feedback (CFB)	Input is processed *s* bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	•General-purpose stream-oriented transmission •Authentication
Output Feedback (OFB)	Similar to CFB, except that the input to the encryption algorithm is the preceding DES output.	•Stream-oriented transmission over noisy channel (e.g., satellite communication)
Counter (CTR)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	•General-purpose block-oriented transmission •Useful for high-speed requirements

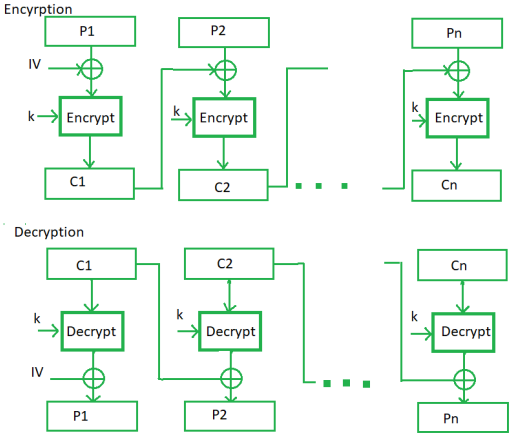
Symmetric Encryption

Block Cipher Modes

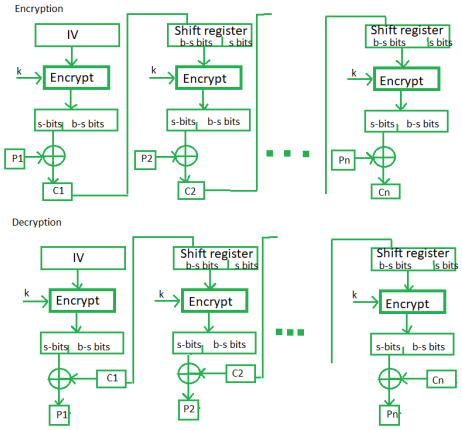
ECB



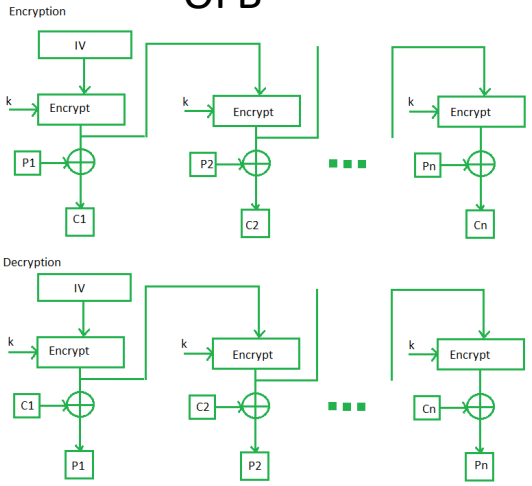
CBC



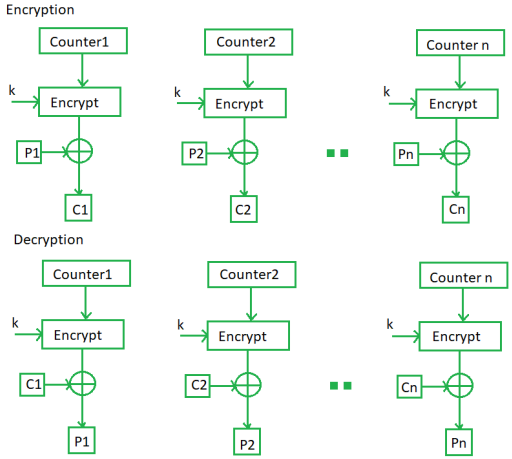
CFB



OFB



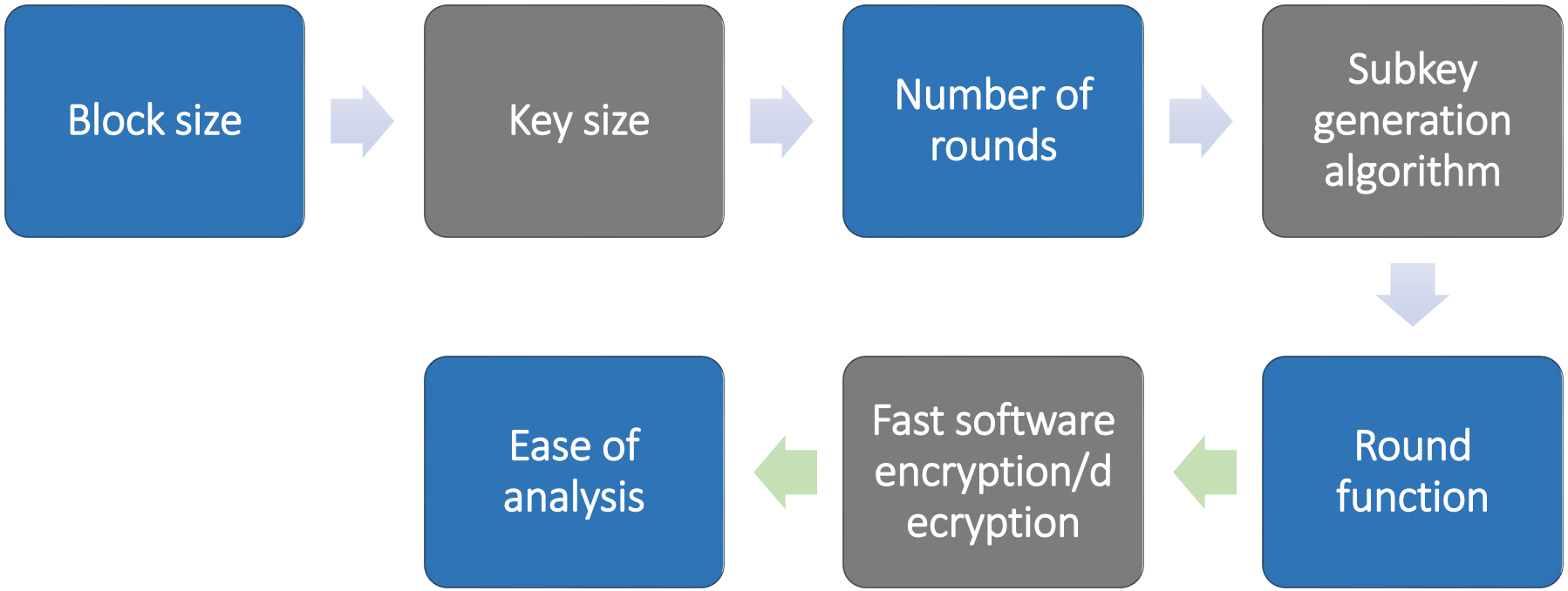
CTR



Symmetric Encryption

Block Cipher

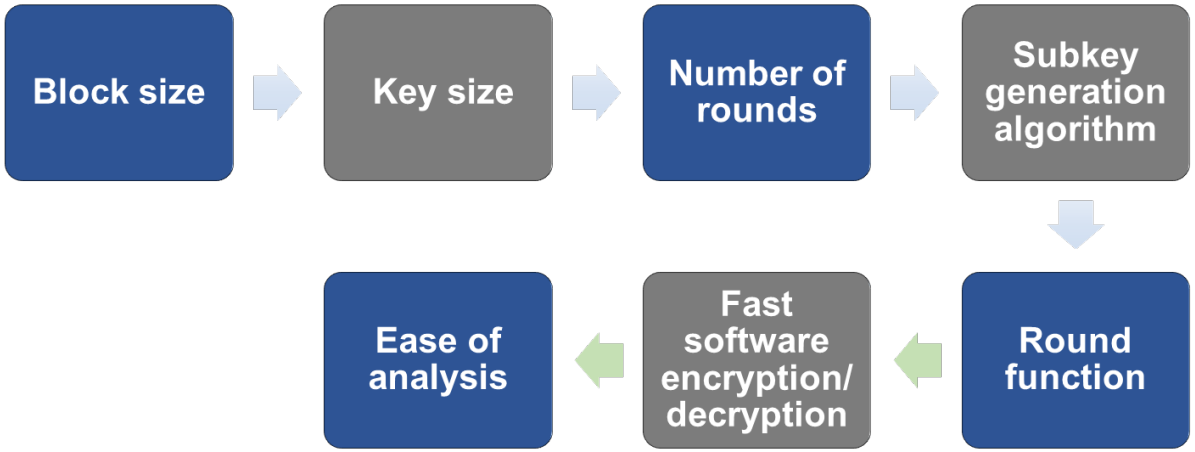
- Processes the input one block of elements at a time
- Produces an output block for each input block
- **Block size:** Larger block sizes mean greater security (all other things being equal) but reduced encryption/decryption speed. A block size of 128 bits is a reasonable trade-off and is nearly universal among recent block cipher designs.



Symmetric Encryption
Block Cipher

- **Key size**: Larger key size means greater security but may decrease encryption/ decryption speed. The most common key length in modern algorithms is 128 bits.
- **Number of rounds**: The essence of a symmetric block cipher is that a single round offers inadequate security but that multiple rounds offer increasing security. A typical size is 16 rounds.
- **Subkey generation algorithm** : Greater complexity in this algorithm should lead to greater difficulty of cryptanalysis.

- **Round function**: Again, greater complexity generally means greater resistance to cryptanalysis.



Symmetric Encryption

Practical Security Issues

- Typically, symmetric encryption is applied to a unit of data larger than a single 64-bit or 128-bit block.
- Electronic codebook (ECB) mode is the simplest approach to multiple-block encryption:
  - Each block of plaintext is encrypted using the same key
  - Cryptanalysts may be able to exploit regularities in the plaintext

Modes of operation:

- Alternative techniques developed to increase the security of symmetric block encryption for large sequences
- Overcomes the weaknesses of ECB

Symmetric Encryption

Characteristics of Popular algorithms

	DES	Triple DES	AES
Plaintext block size (bits)	64	64	128
Ciphertext block size (bits)	64	64	128
Key size (bits)	56	112 or 168	128, 192, or 256

DES = Data Encryption Standard
AES = Advanced Encryption Standard

Symmetric Encryption

Attack Strategy

Cryptanalytic Attacks

- Rely on:
  - Nature of the algorithm
  - Some knowledge of the general characteristics of the plaintext
  - Some sample plaintext-ciphertext pairs
- Exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or the key being used
  - If successful, all future and past messages encrypted with that key are compromised

Brute-force attacks

- Try all possible keys on some ciphertext until an intelligible translation into plaintext is obtained
- On average half of all possible keys must be tried to achieve success
- Number of Keys are dictated by the key size.