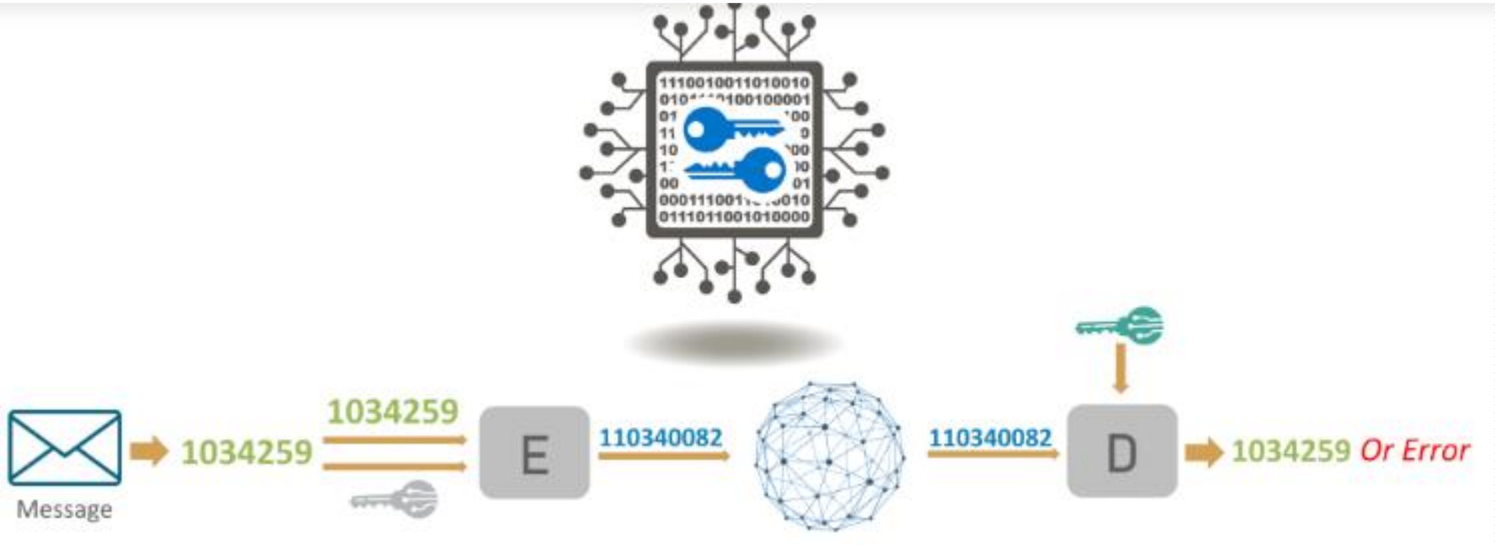
Lecture 4

CRYPTOGRAPH



* << >> ↵

Introduction

- The increased use of computer and communications systems by industry **has increased the risk of theft of proprietary information.**

- Threats may require a variety of countermeasures, **encryption is a primary method of protecting valuable electronic information**.

* << >> ↵

Cryptography

- Cryptography is a method of protecting information and communications through the **use of codes,** so that only those for **whom the information is intended can read and process it.**
- The prefix "**crypt**" means "**hidden**" and suffix **graphy** means "**writing**".
- The important automated tool for network and communications security is encryption.

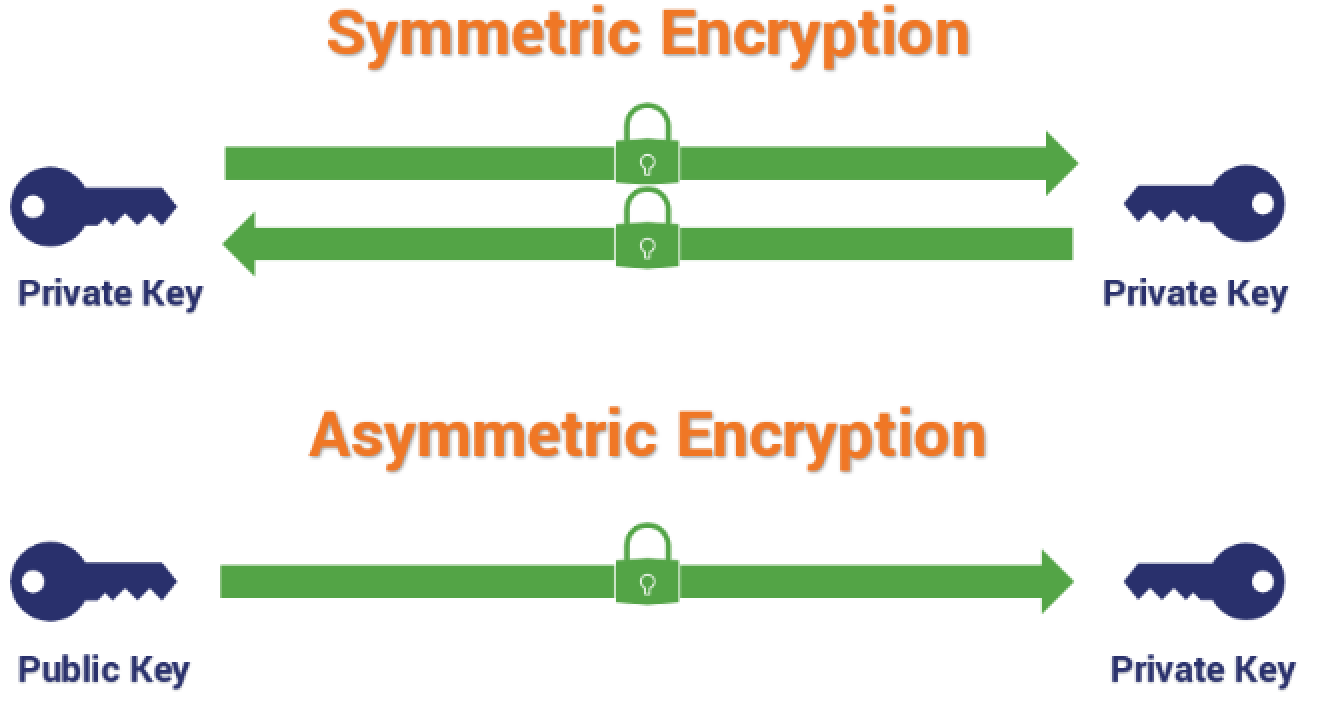
Con’t

- In **computer science**, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called **algorithms**, to **transform messages in ways that are hard to decipher.**
- These deterministic algorithms are used for cryptographic **key generation**, **digital signing**, **verification to protect data privacy**, **web browsing** on the internet and confidential communications such as **credit card transactions** and email.

* << >> ↵

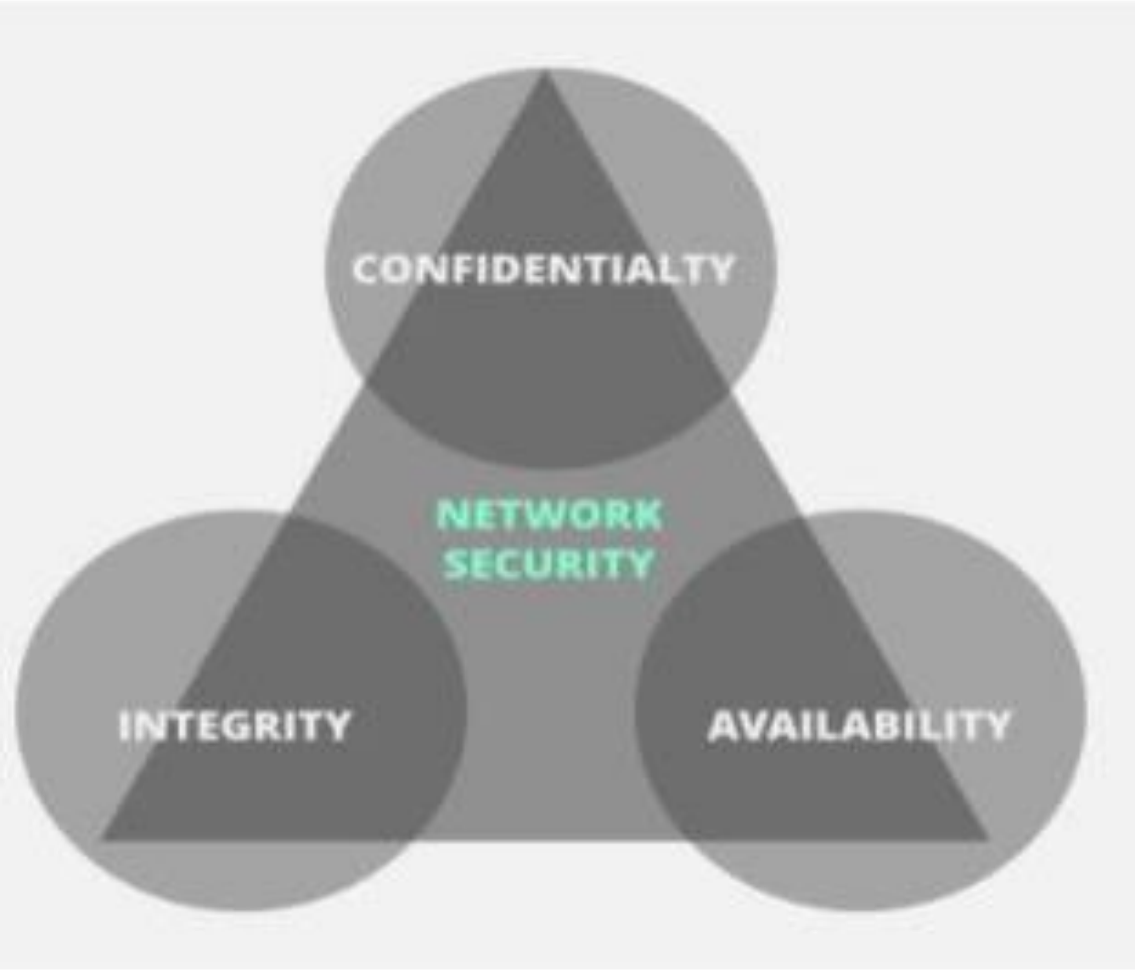
Forms of encryption

1. Conventional or symmetric encryption and
2. Public-key, or asymmetric encryption.



Objectives of Cryptography

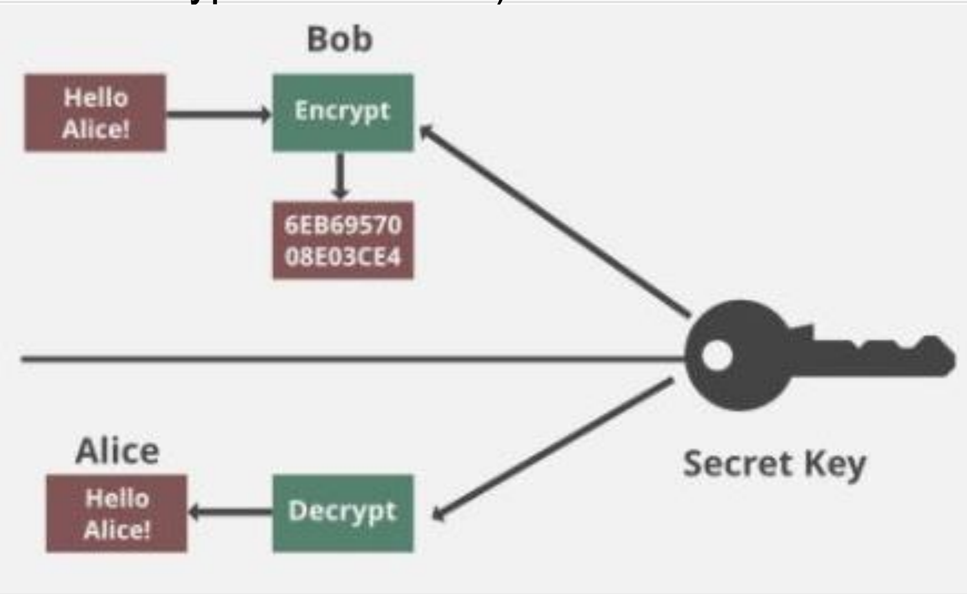
The CIA triad in Cryptography. Confidentiality, Integrity and Availability



Confidentiality

Confidentiality/Authenticity means that only authorized individuals/systems can view sensitive or classified information.

- The data being sent over the network should not be accessed by unauthorized individuals
- Encryption standards include **AES**(Advanced Encryption Standard) and **DES** (Data Encryption Standard).



* << >> ↵

Integrity

- Refers to make sure that data has **not been modified**, **Corruption of data is a failure to maintain data integrity.**

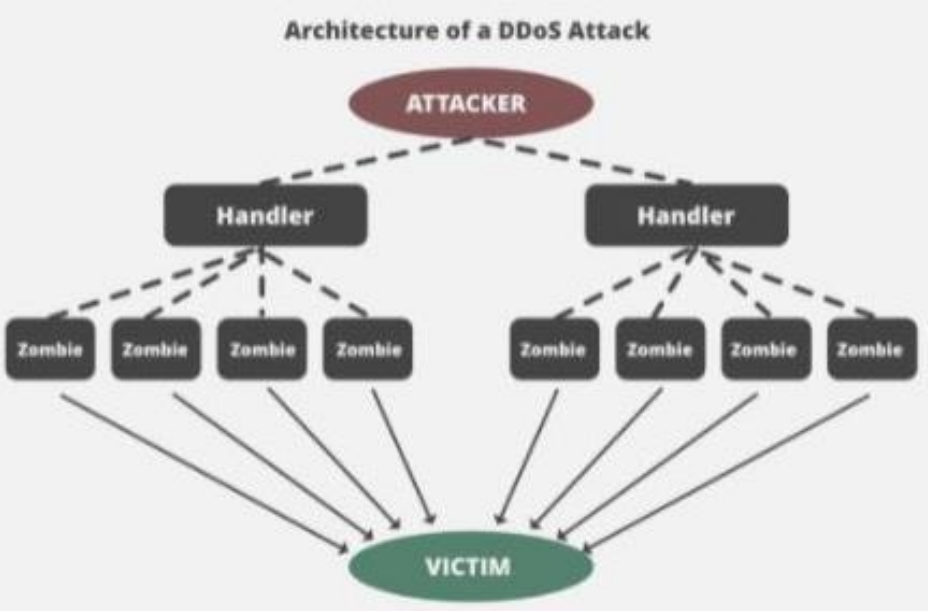
Let's assume **Host 'A'** wants to send data to **Host 'B'** maintaining integrity. A hash function will run over the data and produce an arbitrary hash value **H1** which is then attached to the data. **When Host 'B' receives the packet**, it runs the **same hash function over the data** which gives a hash value **H2**.

Now, if **H1 = H2**, this means that the data's integrity has been maintained and the contents were not modified.

Availability

- This means that the network should be **readily available to its users** (systems and data).
- To ensure availability, the network administrator should maintain **hardware**, **make regular upgrades**, have a plan for fail-over, and prevent bottlenecks in a network.

Attacks such as DoS or DDoS may render a network unavailable as the resources of the network get exhausted.



Types of Cryptography Techniques

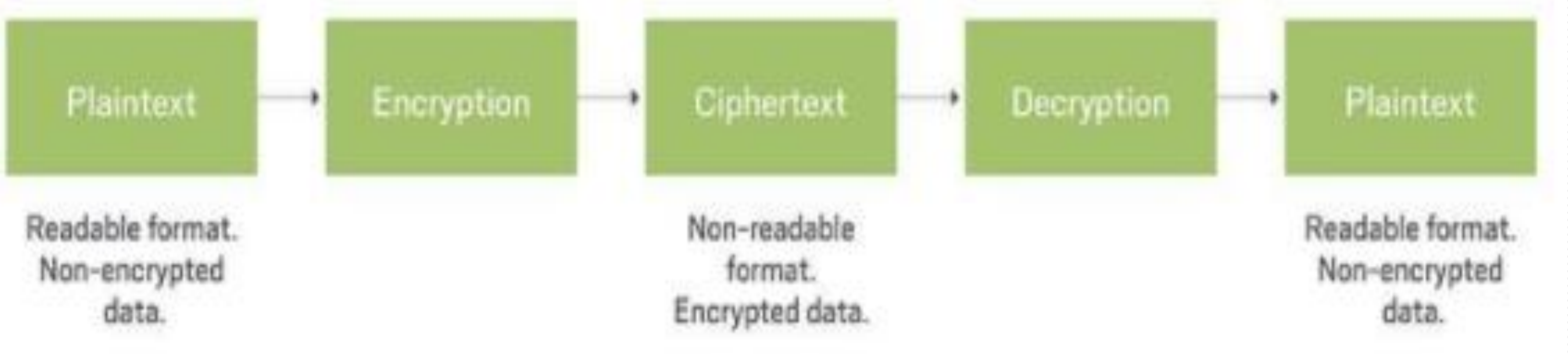
Cryptography can be broken down into three different types:

1. Secret Key Cryptography
2. Public Key Cryptography
3. Hash Functions

* << >> ↵

Symmetric Cipher Model

A symmetric encryption scheme has five ingredients


Plaintext
Encryption
Ciphertext
Decryption
Plaintext
Readable format. Non-encrypted data.
Non-readable format. Encrypted data.
Readable format. Non-encrypted data.

1. Plaintext:
2. Encryption algorithm:.
3. Secret key.
4. Ciphertext:
5. Decryption algorithm

Con’t

Plaintext: This is the original intelligible message or data that is fed into the algorithm as input.

Encryption algorithm: It performs various substitutions and transformations on the plaintext.

Secret key: It is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. **The algorithm will produce a different output depending on the specific key being used at the time.**

* << >> ↵

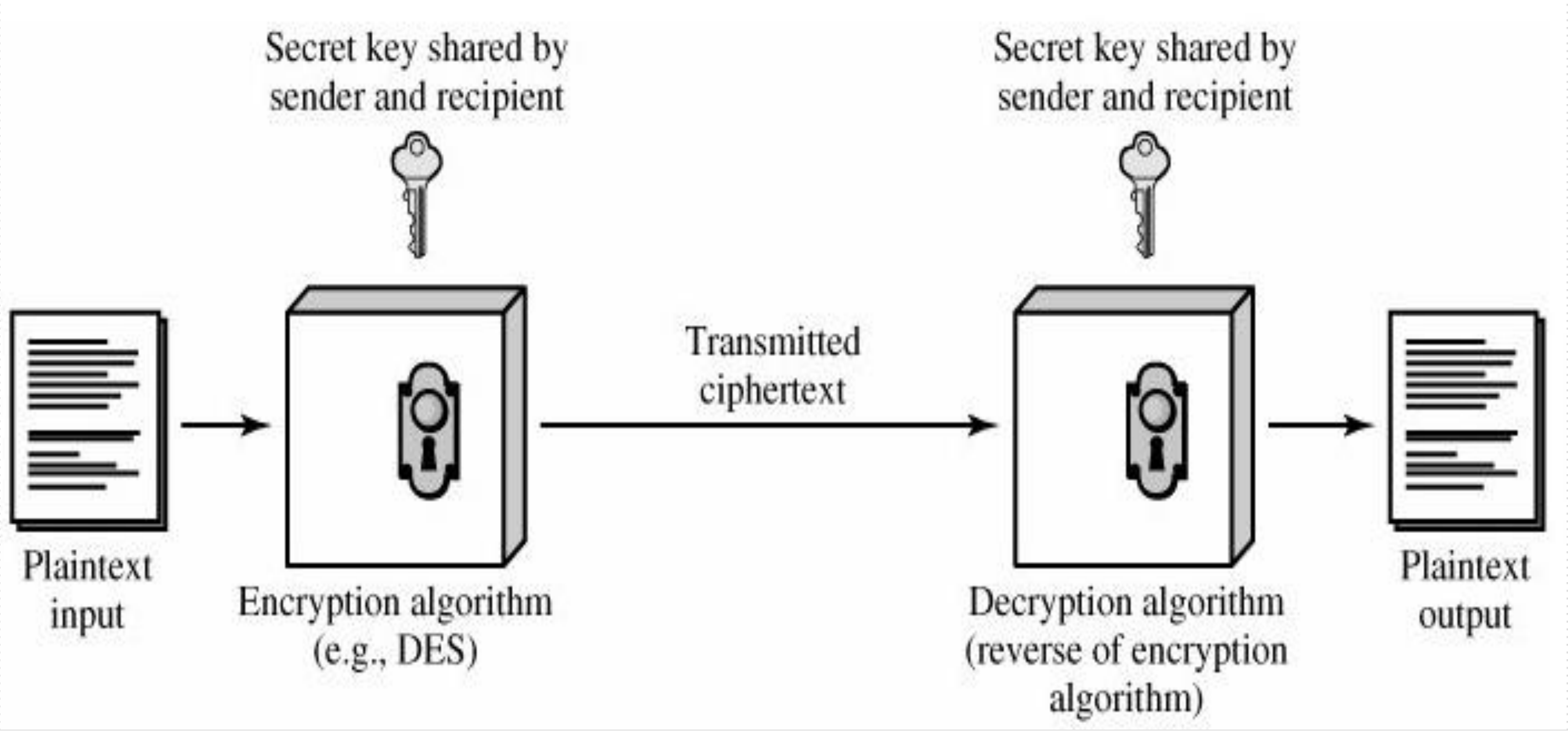
Con’t

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. The cipher text is an apparently random stream** of data and, as it stands, is unintelligible.

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

* << >> ↵

Model of Conventional Encryption


Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

* << >> ↵

Requirements of conventional encryption

- **Two requirements for secure use of conventional encryption:**

1. **We need a strong encryption algorithm.** At a minimum, we would like the algorithm to be such that an opponent who knows the algorithm and has access to one or more cipher texts would be unable to decipher the ciphertext or figure out the key. **This requirement is usually stated in a stronger form:** The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertexts .

* << >> ↵

Con’t

2. **Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.** If someone can discover the key and knows the algorithm, all communication using this key is readable

* << >> ↵

Secret Key Cryptography

Secret/**Symmetric** Key Cryptography;

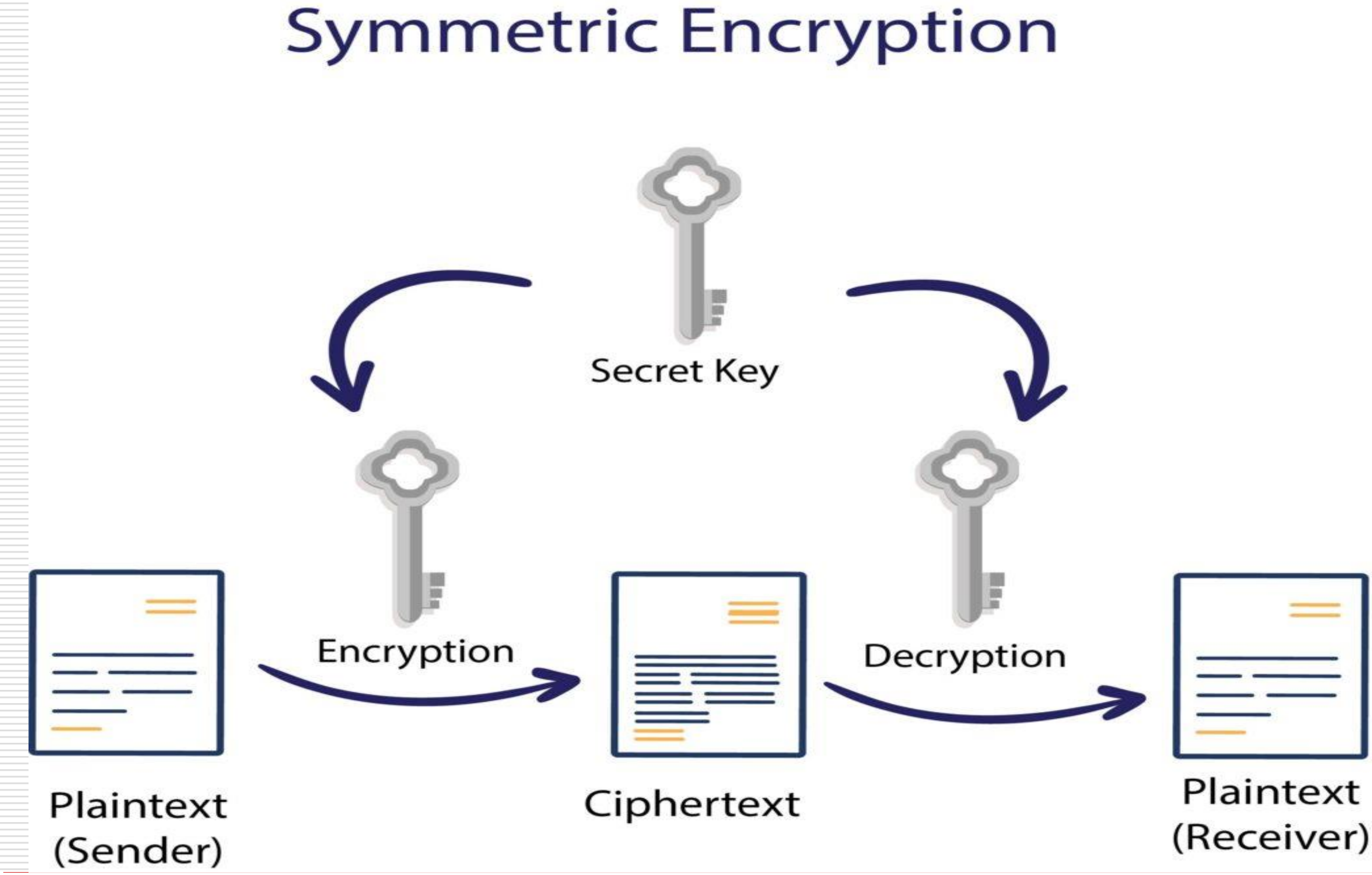
- Uses a single key to encrypt data.
- Both encryption and decryption in symmetric cryptography use the same key, making this the easiest form of cryptography.

Examples:

1. **AES**
2. **DES**
3. **Caesar Cipher**

* << >> ↵

Symmetric Encryption



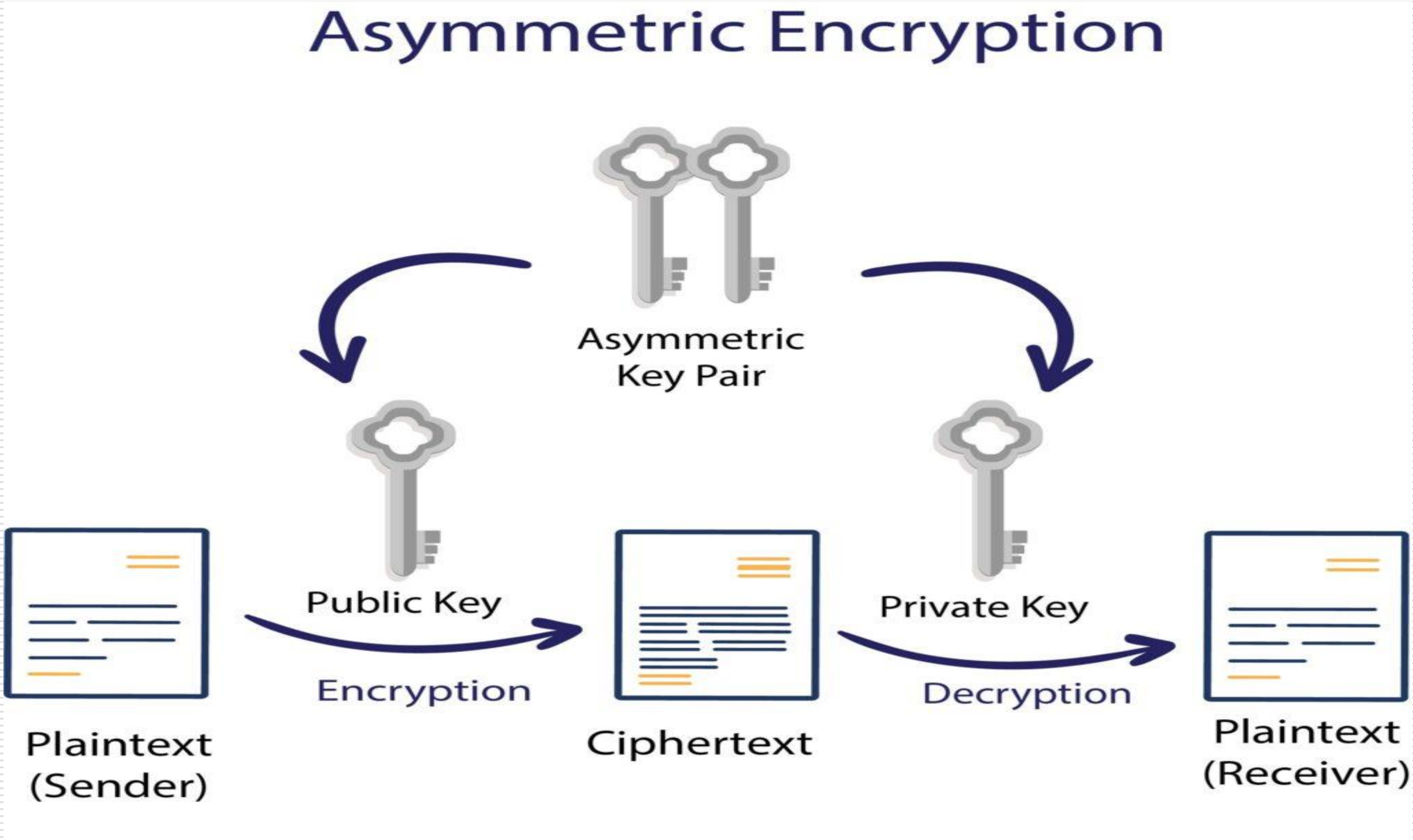
Public Key Cryptography

Public/ asymmetric Key Cryptography,

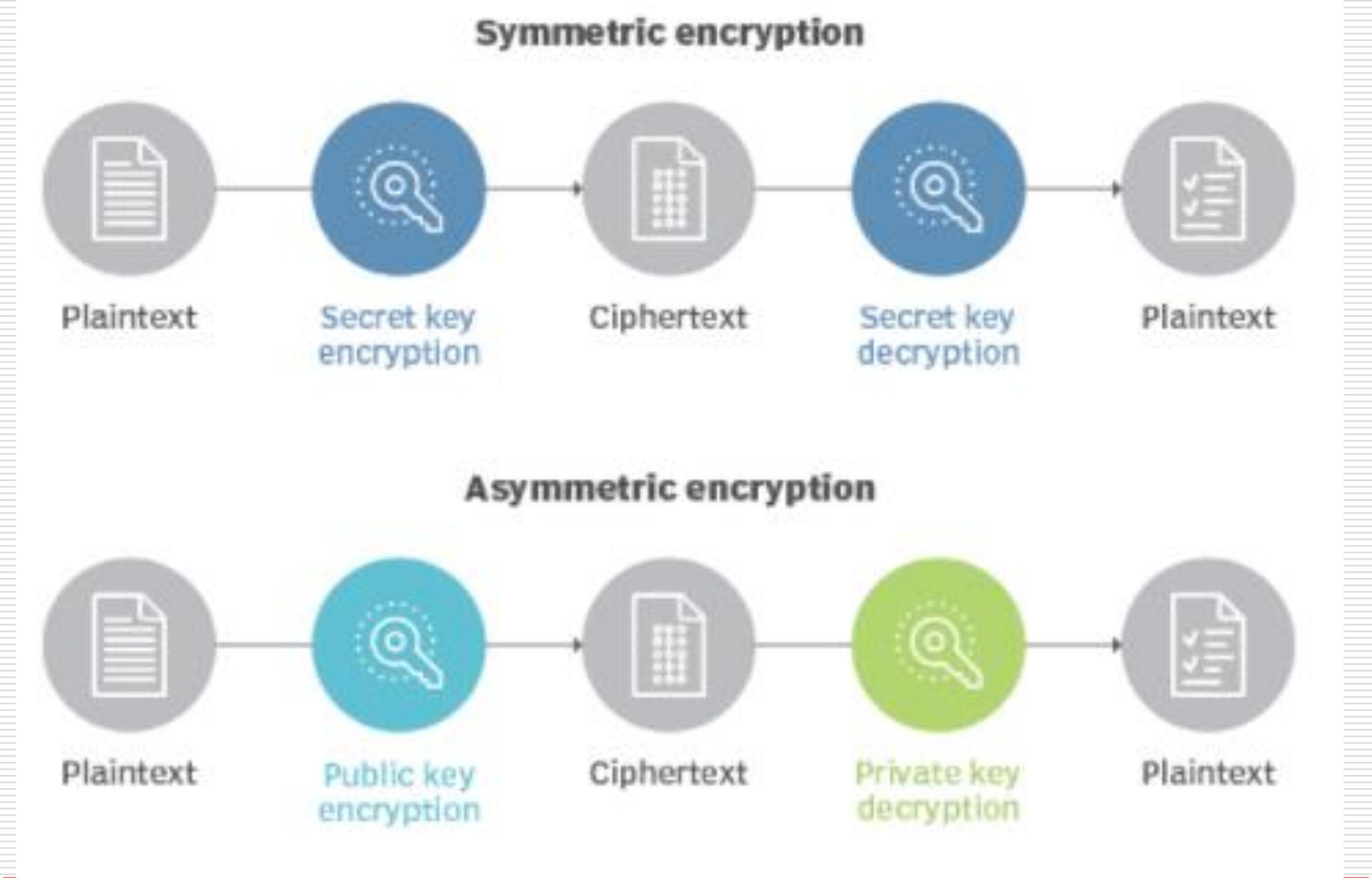
- Uses two keys to encrypt data.
- **One is used for encryption**, while the **other key can decrypts the message**.
- Unlike symmetric cryptography, if one key is used to encrypt, that same key cannot decrypt the message, rather the other key shall be used.

* << >> ↵

Asymmetric Encryption



Symmetric Vs Asymmmetric Encryption



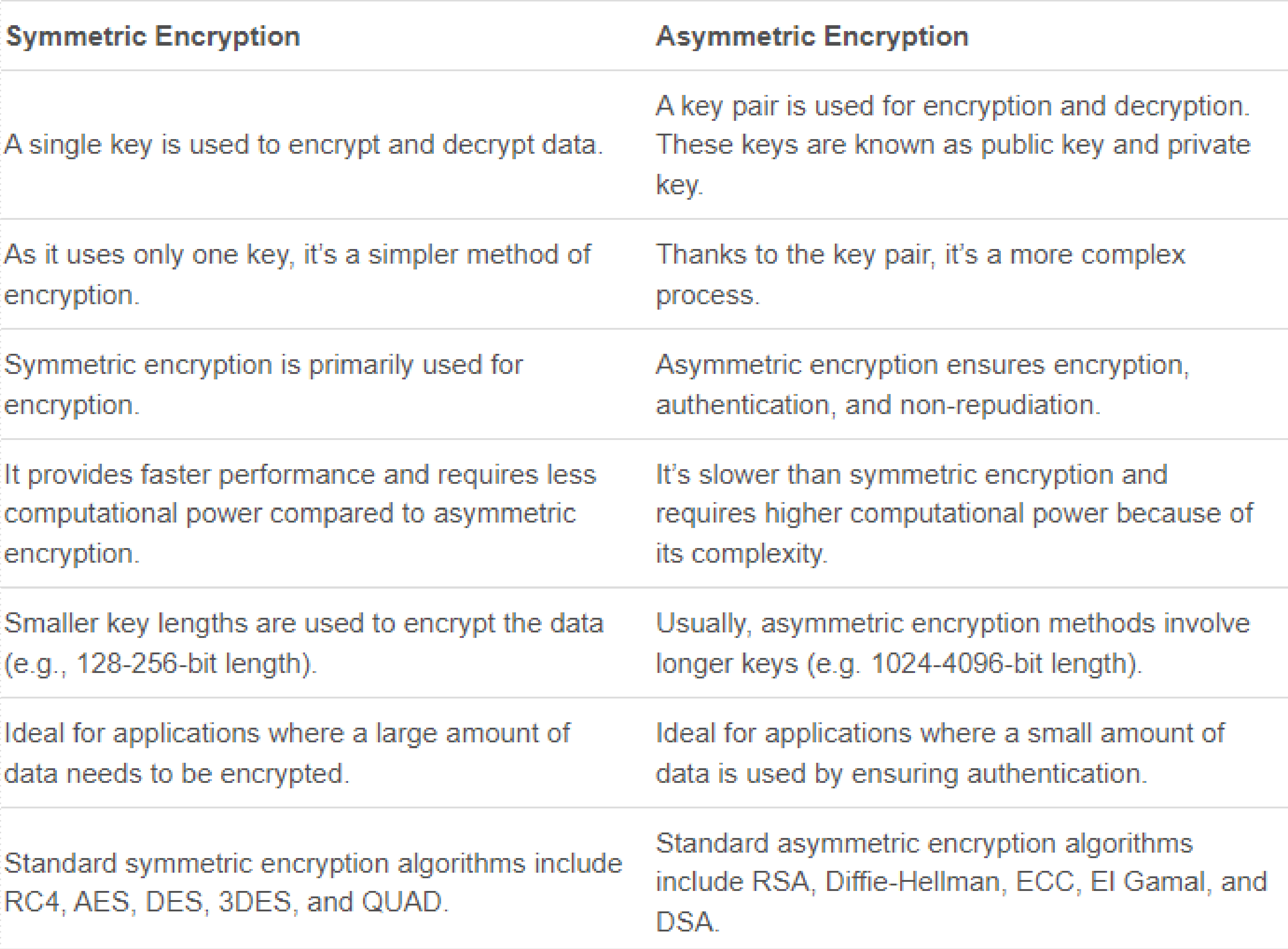
Con’t

- One key is kept private, and is called the “**private key**”, while the other is shared publicly and can be used by anyone, hence it is known as the “**public key**”.
- The mathematical relation of the keys is such that the private key cannot be derived from the public key, but the public key can be derived from the private.
- The private key **should not be distributed** and **should remain with the owner only**. The public key can be given to any other entity.

Examples:

1. ECC_Elliptic curve cryptography
2. Diffie-Hellman
3. DSS_Digital Signature Standard

* << >> ↵



Symmetric Encryption	**Asymmetric Encryption**
A single key is used to encrypt and decrypt data.	A key pair is used for encryption and decryption. These keys are known as public key and private key.
As it uses only one key, it's a simpler method of encryption.	Thanks to the key pair, it's a more complex process.
Symmetric encryption is primarily used for encryption.	Asymmetric encryption ensures encryption, authentication, and non-repudiation.
It provides faster performance and requires less computational power compared to asymmetric encryption.	It's slower than symmetric encryption and requires higher computational power because of its complexity.
Smaller key lengths are used to encrypt the data (e.g., 128-256-bit length).	Usually, asymmetric encryption methods involve longer keys (e.g. 1024-4096-bit length).
Ideal for applications where a large amount of data needs to be encrypted.	Ideal for applications where a small amount of data is used by ensuring authentication.
Standard symmetric encryption algorithms include RC4, AES, DES, 3DES, and QUAD.	Standard asymmetric encryption algorithms include RSA, Diffie-Hellman, ECC, El Gamal, and DSA.

Hash functions

Hash functions are irreversible, one-way functions which protect the data, at the cost of not being able to recover the original message.

Hashing is a way to transform a given string into a fixed length string. A good hashing algorithm will produce unique outputs for each input given.

The only way to crack a hash is by trying every input possible, until you get the exact same hash. A hash can be used for hashing data (such as **passwords**) and in certificates.

Con’t

Some of the most famous hashing algorithms are:

1. MD5(**M**essage**-D**igest algorithm)
2. SHA-1(Secure Hash **Algorithm** 1)
3. SHA-2 family which includes SHA-224, SHA-256, SHA-384, and SHA-512
4. SHA-3
5. Whirlpool
6. Blake 2
7. Blake 3

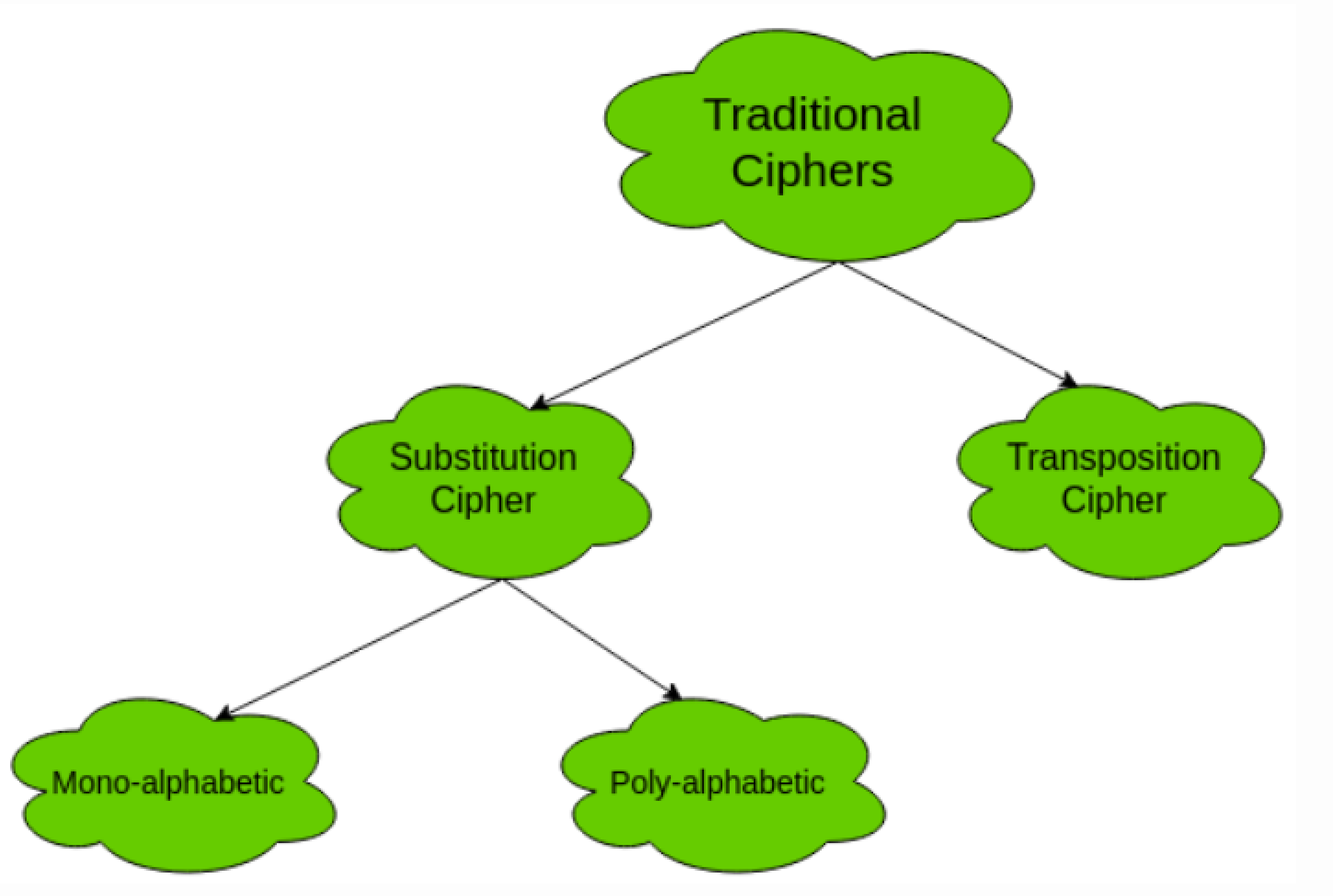
* << >> ↵

Classical Encryption Techniques

- This techniques enables us to illustrate the basic approaches **to symmetric encryption used today** and the types of cryptanalytic attacks that must be anticipated.
- The two basic building blocks of all encryption techniques are **substitution** and **transposition.**

* << >> ↵

Types of traditional symmetric ciphers



Substitution Techniques

- A **substitution technique** is one in which the **letters of plaintext are replaced by other letters or by numbers or symbols.** If the plaintext is viewed as a **sequence of bits**, then substitution involves replacing plaintext bit patterns with cipher text bit patterns.
- In a substitution cipher **each letter** or **group of letters** is replaced by another letter or group of letters to disguise it.
- ciphers is the **Caesar cipher**, attributed to **Julius Caesar, 49 BC**. In this method, **a becomes D**, **b becomes E**, **c becomes F**, ... , and **z becomes C**. In examples, **plaintext will be given in lower case letters**, and **ciphertext in upper case letters.**

* << >> ↵

Caesar Cipher

- It is a **mono-alphabetic cipher** wherein each letter of the plaintext is substituted by another letter to form the cipher text. It is a simplest form of substitution cipher scheme.
- A **substitution cipher scheme,** and is the simplest form, was introduced by **Julius Caesar, 49BC.**
- This cryptosystem is generally referred to as the **Shift Cipher**. The concept is to replace each alphabet by another alphabet which is '**shifted**' by some fixed **number between 0 and 25**.

* << >> ↵

Con’t

For example,

- **plain: meet me after the toga party**
- **cipher: PHHW PH DIWHU WKH WRJD SDUWB**

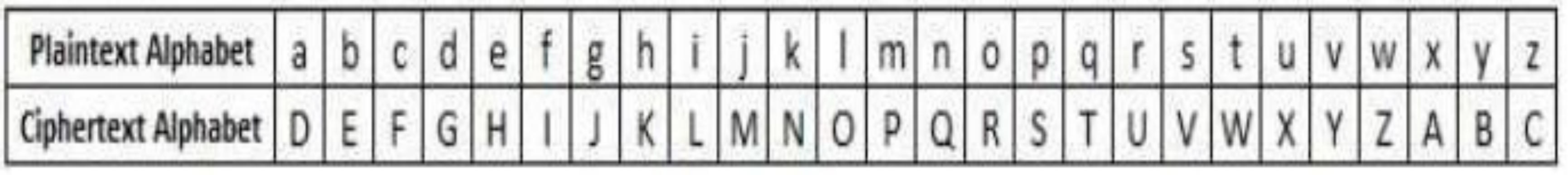
*Note that the alphabet is wrapped around, so that the letter **following Z is A**. We can define the transformation by listing all possibilities, as follows:*

plain: 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

cipher: 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**

Process of Shift Cipher

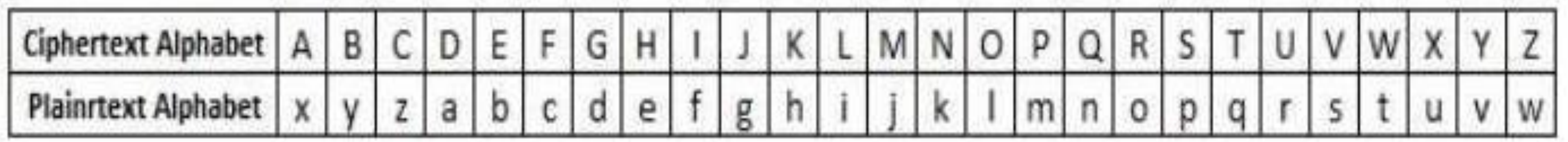
- In order to encrypt a plaintext letter, the **sender positions the sliding ruler underneath the first set** of plaintext letters and slides it to **LEFT** by the number of positions of the secret shift.
- The plaintext letter is then encrypted to the **cipher text** letter on the sliding ruler underneath. The result of this process is depicted in the following illustration for an agreed shift of three positions. In this case, the plaintext ‘**tutorial**’ is encrypted to the ciphertext ‘**WXWRULDO**’. Here is the ciphertext **alphabet for a Shift of 3** –



Plaintext Alphabet	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
Ciphertext Alphabet	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

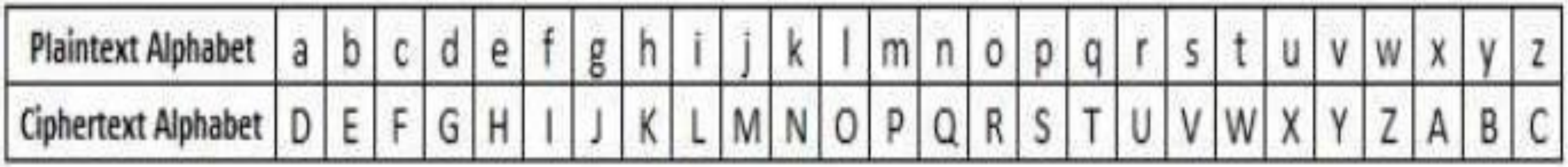
Con’t

- On receiving the ciphertext, the receiver who also knows **the secret shift**, positions his sliding ruler underneath the ciphertext alphabet and slides it to **RIGHT** by the agreed **shift number, 3 in this case**.
- He then replaces the **ciphertext letter by the plaintext letter** on the sliding ruler underneath. Hence the ciphertext ‘**WXWRULDO**’ is decrypted to ‘**tutorial**’. To decrypt a message encoded **with a Shift of 3,** generate the plaintext alphabet using a shift of ‘-3’ as shown below –



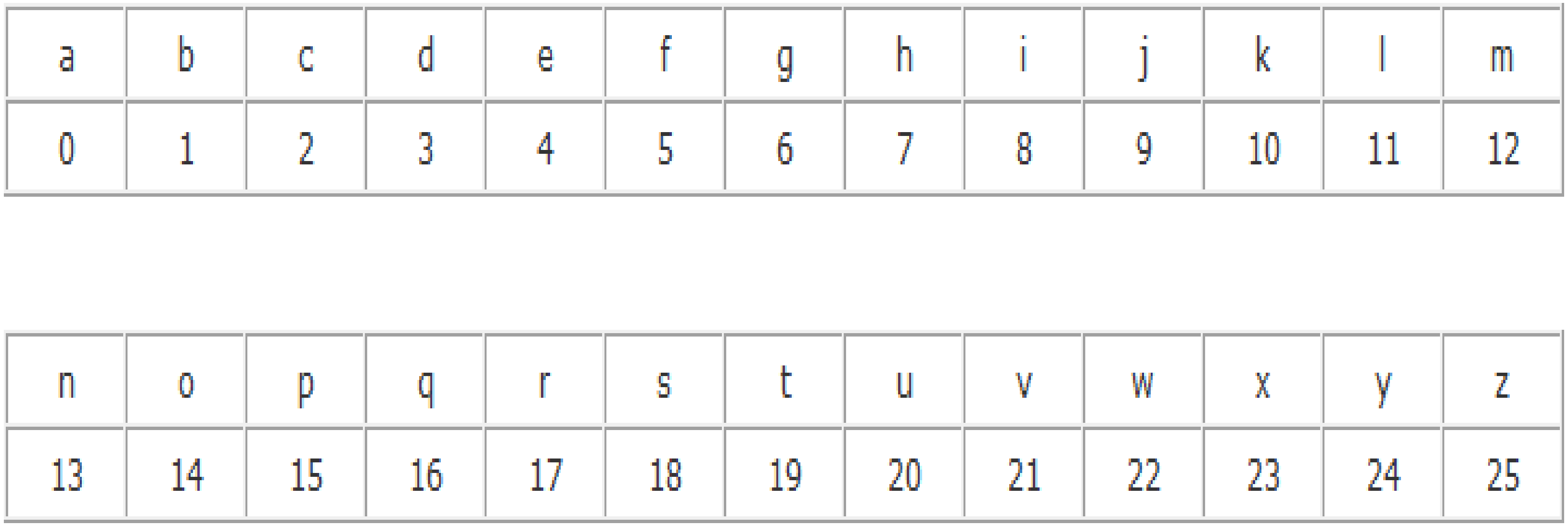
Ciphertext Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Plainrtext Alphabet	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w

Con’t



Plaintext Alphabet	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
Ciphertext Alphabet	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

Let us assign a numerical equivalent to each letter



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

* << >> ↵

Algorithm

Then the algorithm can be expressed as follows**. For** each **plaintext letter (p),** substitute the **ciphertext letter (C).**

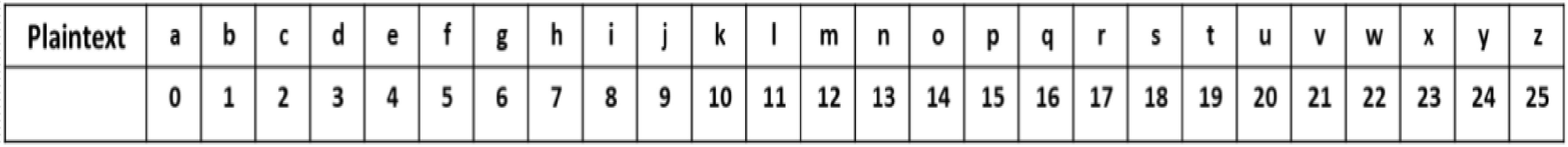
- $C = E(k, p) = (p + 3) \bmod 26$, A shift may be of any amount, so that the general **Caesar algorithm** is:
- **Encryption**: $C = E(k, p) = (p + k) \bmod 26$ **.........(1)** Where “**k**” takes on a value in the range **1 to 25**.
- **Decryption**: $p = D(k, C) = (C - k) \bmod 26$ **.........(2)**

* << >> ↵

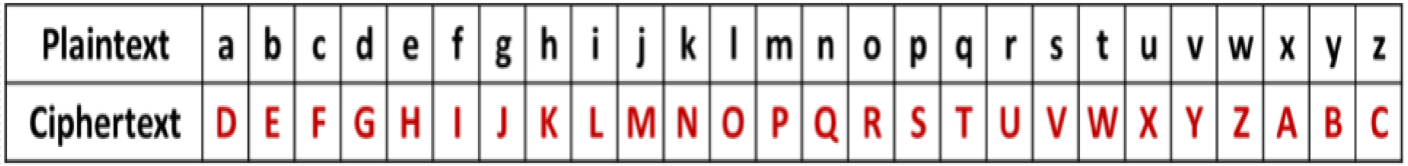
Con’t

Example#1: Encrypt the message **“meet me after the toga party”** , using Caesar cipher.

Ans. : C = E(k, p) = (p + 3) mod 26



Plaintext	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
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25



Plaintext	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
Ciphertext	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

Sol:

The ciphertext C: “PHHW PH DIWHU WKH WRJD SDUWB”

* << >> ←

Con’t

Example#2: Encrypt the message **“ohio state”** , using Caesar cipher.

- **Ans. :** The ciphertext **C: “RKLR VWDWH”**

Example#3:

- Decrypt the ciphertext **“PHHW PH DIWHU WKH WRJD SDUWB”** , using Caesar cipher**.**
- **Ans. : p = D(k, C) = (C - k) mod 26**
- The plaintext**: “meet me after the toga party”**

* << >> ↵

Monoalphabetic Cipher

- **Monoalphabetic** cipher is a substitution cipher in which for a given key, the cipher alphabet for each plain alphabet is fixed throughout the encryption process. For example, if **‘A’ is encrypted as ‘D’,** for any number of occurrence in that plaintext, **‘A’ will always get encrypted to ‘D’.**
- With only 25 possible keys, **the Caesar cipher is far from secure**. A dramatic increase in the key space can be achieved by allowing an arbitrary substitution. Recall the assignment for the Caesar cipher:

plain: 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

cipher: 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

* << >> ↵

Con’t

- If, instead, the "**cipher**" line can be any **permutation** of the 26 alphabetic characters, then there are 26! or greater than 4 x 10^{26} possible keys. This is 10 orders of magnitude greater than the key space for DES and would seem to eliminate brute-force techniques for cryptanalysis. Such an approach is referred to as **a monoalphabetic substitution** cipher, because a single cipher alphabet (mapping from plain alphabet to cipher alphabet) is used per message.

Polyalphabetic Cipher

- It is an improvement of simple monoalphabetic technique is to use different monoalphabetic substitutions as one proceeds through the plaintext message.
- The general name for this approach is **polyalphabetic** substitution cipher.
- Polyalphabetic Cipher is a substitution cipher in which the cipher alphabet for the plain alphabet may be different at different places during the encryption process. The next two examples, **playfair and Vigenere Cipher**

* << >> ↵

A. Play fair Cipher

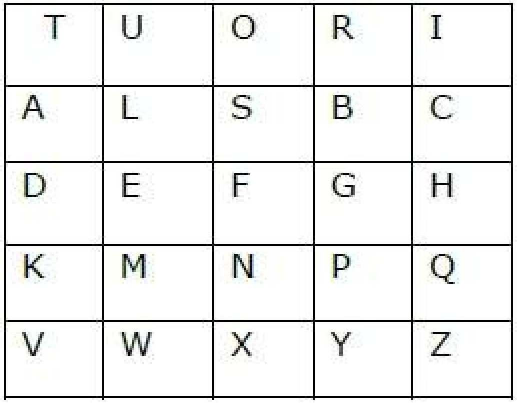
- In this scheme, **pairs of letters are encrypted**, instead of single letters as in the case of **simple substitution cipher.**
- **In play fair cipher**, initially a key table is created. **The key table is a 5×5 grid of alphabets** that acts as the key for encrypting the plaintext.
- Each of the **25 alphabets must be unique** and one letter of the alphabet (usually J) is omitted from the table as we need only 25 alphabets instead of 26**. If the plaintext contains J, then it is replaced by I.**

Con’t

- The **sender** and the **receiver** deicide on a particular key, say ‘**tutorials**’.
- In a key table, the first characters (**going left to right**) in the table is the phrase, excluding the **duplicate letters**.
- The rest of the table will be filled with the remaining letters of the alphabet, **in natural order.**

* << >> ↵

Process of Playfair Cipher



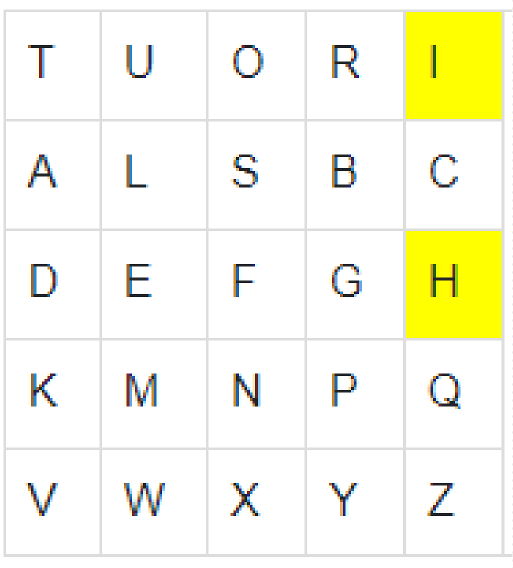
T	U	O	R	I
A	L	S	B	C
D	E	F	G	H
K	M	N	P	Q
V	W	X	Y	Z

- A plaintext message is split into pairs of two letters (**digraphs**). If there is an odd number of letters, a **Z is added to the last letter**. Let us say we want to encrypt the message “**hide money**”. It will be written as –

HI DE MO NE YZ

The rules of encryption

If both the letters are in the **same column**, take the letter below each one (**going back to the top if at the bottom**)



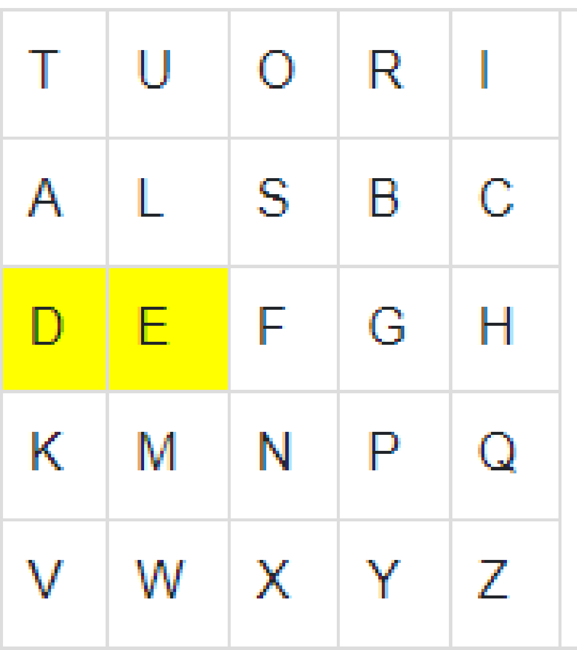
T	U	O	R	I
A	L	S	B	C
D	E	F	G	H
K	M	N	P	Q
V	W	X	Y	Z

‘H’ and ‘I’ are in same column, hence take letter below them to replace.

HI → QC

The rules of encryption-Con’t

If both letters are in **the same row,** take the letter to the right of each one (**going back to the left if at the farthest right)**



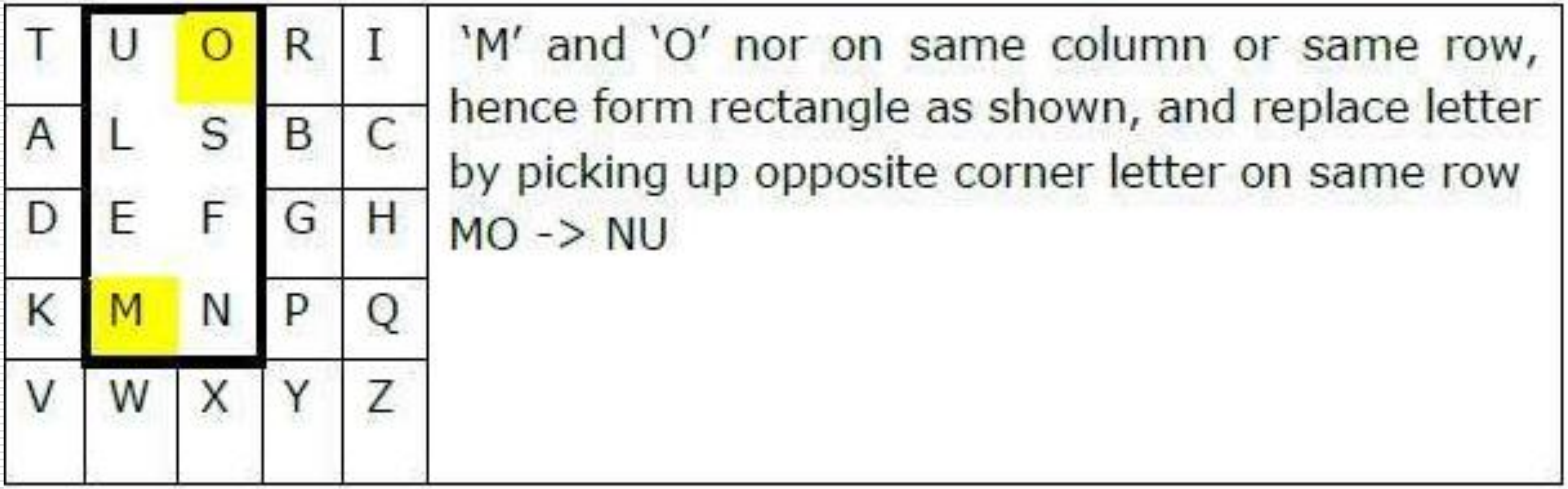
T	U	O	R	I
A	L	S	B	C
D	E	F	G	H
K	M	N	P	Q
V	W	X	Y	Z

‘D’ and ‘E’ are in same row, hence take letter to the right of them to replace.

DE → EF

The rules of encryption-Con’t

If neither of the preceding **two rules are true**, **form a rectangle** with the two letters and **take the letters on the horizontal opposite corner of the rectangle**.



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

‘M’ and ‘O’ nor on same column or same row, hence form rectangle as shown, and replace letter by picking up opposite corner letter on same row MO -> NU

Using these rules, the result of the encryption of ‘**hide money**’ with the key of ‘tutorials’ would be −**QC EF NU MF ZV**

Decrypting the Playfair cipher is as simple as doing the same process in reverse.

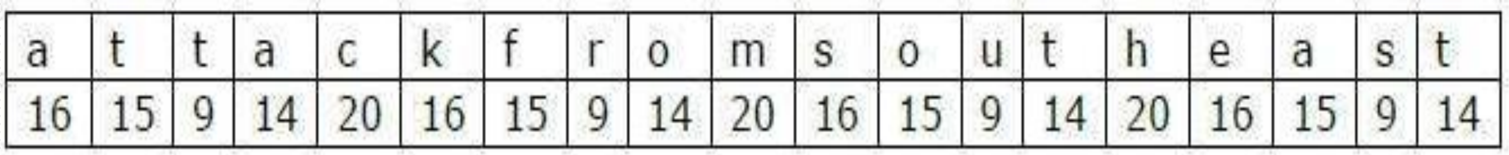
Receiver has the same key and can create the same key table, and then decrypt any messages made using that key.

B. Vigenere Cipher

- This scheme of cipher uses a text string (say, **a word**) **as a key**, which is then used for doing a number **of shifts on the plaintext.**
- For example, let’s assume the key is ‘**point**’. Each alphabet of the key is converted to its respective numeric value: In this case,
- **p → 16, o → 15, i → 9, n → 14, and t → 20.**
- Thus, the key is: 16 15 9 14 20.

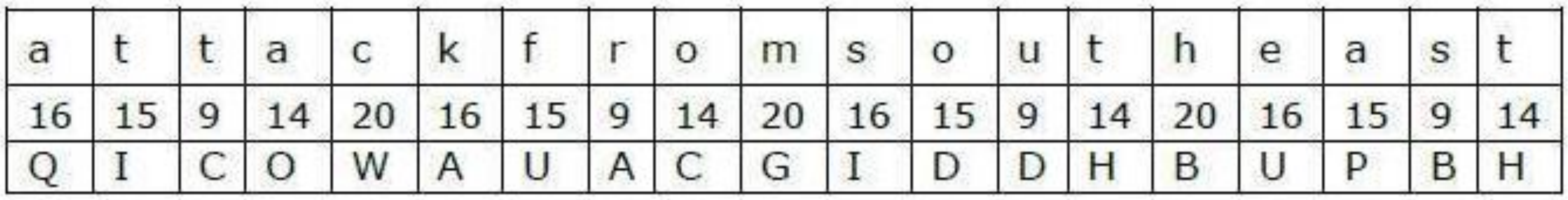
Process of Vigenere Cipher

- The **sender and the receiver** decide on a key. Say ‘**point**’ is the key. Numeric representation of this key is ‘**16 15 9 14 20**’.
- The sender wants to encrypt the message, say ‘**attack from south east**’. He will arrange plaintext and numeric key as follows



a	t	t	a	c	k	f	r	o	m	s	o	u	t	h	e	a	s	t
16	15	9	14	20	16	15	9	14	20	16	15	9	14	20	16	15	9	14

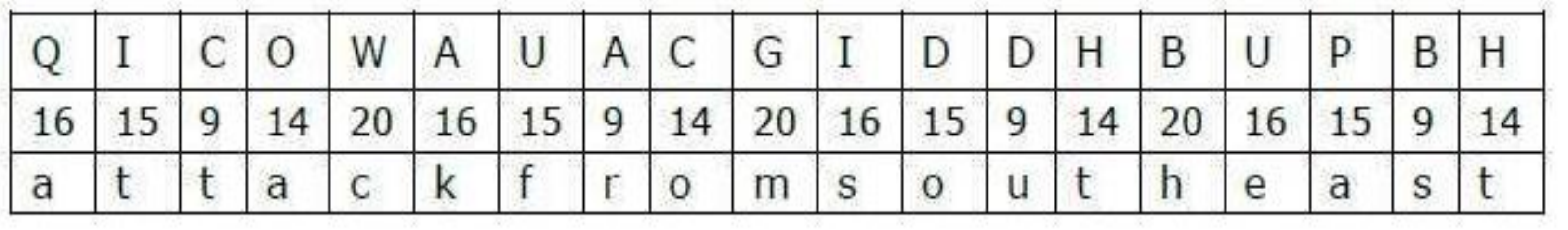
- He now **shifts each plaintext alphabet by the number written** below it to create cipher text as shown below



a	t	t	a	c	k	f	r	o	m	s	o	u	t	h	e	a	s	t
16	15	9	14	20	16	15	9	14	20	16	15	9	14	20	16	15	9	14
Q	I	C	O	W	A	U	A	C	G	I	D	D	H	B	U	P	B	H

Con’t

- Here, **each plaintext character has been shifted by a different amount** – and **that amount is determined by the key.** The key must be less than or equal to the size of the message.
- For decryption, the receiver uses the same key and shifts received cipher **text in reverse order to obtain** the plaintext.



Q	I	C	O	W	A	U	A	C	G	I	D	D	H	B	U	P	B	H
16	15	9	14	20	16	15	9	14	20	16	15	9	14	20	16	15	9	14
a	t	t	a	c	k	f	r	o	m	s	o	u	t	h	e	a	s	t

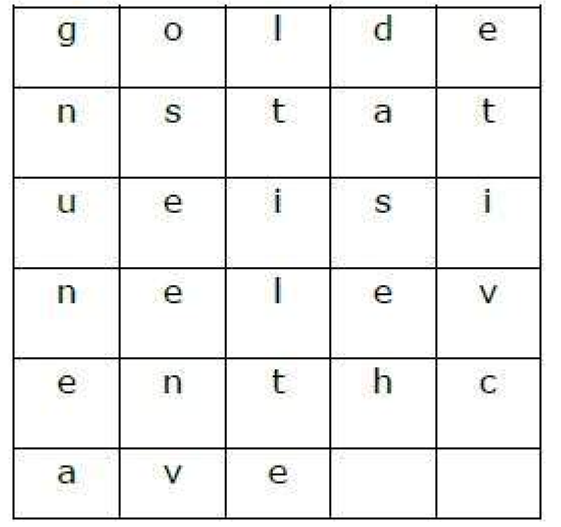
There are two special cases of Vigenere cipher – **Vernam Cipher**. And **One-time pad**.

Transposition Ciphers

- It is **a type of cipher** where the order of the alphabets in the plaintext is **rearranged** to create the ciphertext. The actual plaintext alphabets are not replaced.
- An example is a ‘**simple columnar transposition**’ cipher where the plaintext is **written horizontally** with a certain alphabet width. **Then the ciphertext is read vertically**
- For example, the plaintext is **“golden statue is in eleventh cave**” and the secret random key chosen is “**five**”. We arrange this **text horizontally** in table with number of **column equal to key value**. The resulting text is shown below.

* << >> ↵

Transposition



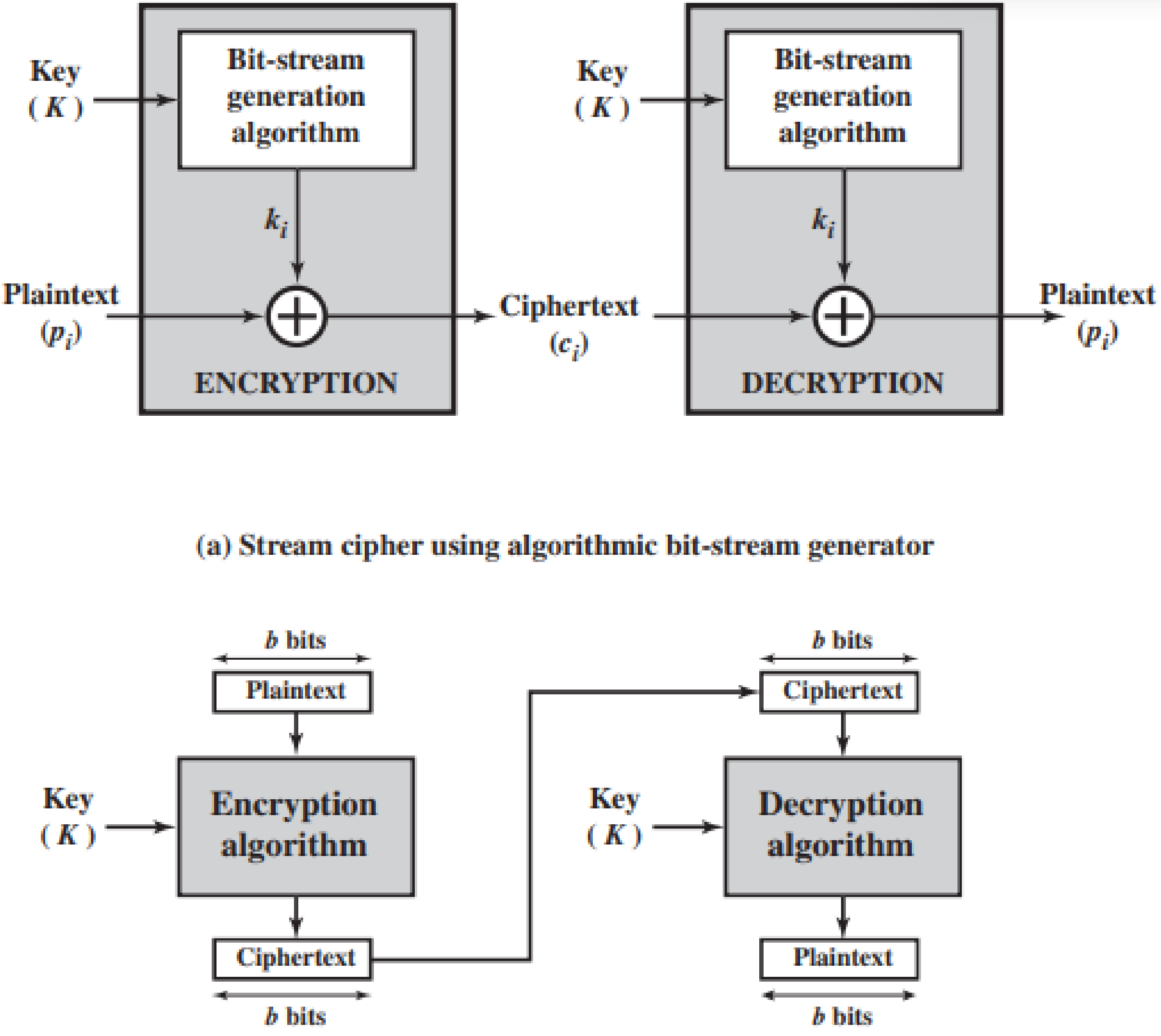
g	o	l	d	e
n	s	t	a	t
u	e	i	s	i
n	e	l	e	v
e	n	t	h	c
a	v	e		

- The cipher text is obtained by reading **column vertically downward from** first to last column. The cipher text is **‘gnuneaoseenvltiltedasehetivc**’.
- **To decrypt**, the receiver prepares similar table. The number of columns is equal to **key number. The number of rows is obtained by dividing number of total cipher text alphabets by key value and rounding of the quotient to next integer value.**
- The receiver then writes the received cipher text **vertically down** and from **left to right column.**
- To obtain the text, he reads **horizontally left to right and from top to bottom** row.

Stream Vs Block Ciphers

- **A stream Cipher** is one that encrypts a digital data stream one bit or one byte at a time.
- **A block cipher is** one in which a block of plaintext is treated as a whole and used to produce a ciphertext **block of equal length.** Typically, a block size of 64 or 128 bits is used. a block cipher can be used to achieve the same effect as a stream cipher.

Stream Vs Block Ciphers



(a) Stream cipher using algorithmic bit-stream generator

(b) Block cipher

Review Questions

1. What is cryptography?
2. What are the form of encryption ?
3. What are the objectives of cryptography?
4. Differentiate Symmetric from Asymmetric cipher ?
5. Explain the elements of symmetric Cipher Model?
6. Differentiate stream cipher from Block Cipher ?

* << >> ↵

Quiz#2 _ 20Mins

Encrypt your names by using cesaer Cipher

* << >> ↵

Thank You