**أولًا: الأسئلة المتعلقة بخوارزميات التشفير:**

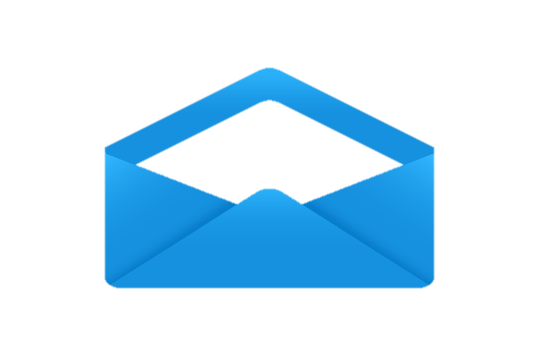
**1- ما الغرض الأساسي من استخدام خوارزميات التشفير؟**

**Encryption** is a technology that works by scrambling data (encrypting your sensitive data) so it is unreadable by unintended parties.[1]

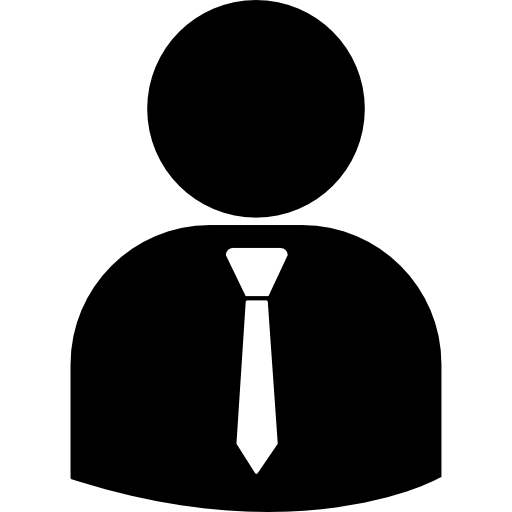
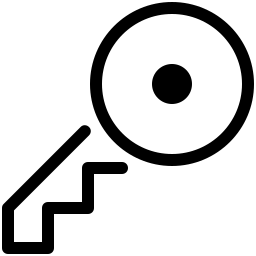
**2- بشرح مبسط و واضح اشرح كيف تعمل خوارزمية التشفير (لك حرية اختيار طريقة الشرح إما بالرسم أو بالوصف).**

3-Sending msg

Encrypt with Key



**wUwDPglyJu9LOnkBAf4vxSpQgQZltcz7LWwEquhdm5kSQIkQlZtfxtSTsmawq6gVH8SimlC3W6TDOhhL2FdgvdIC7sDv7G1Z7pCNzFLp0lgB9ACm8r5R  
N5ske9cBVjlVfgmQ9VpFzSwzLLODhCU7/2THg2iDrW3NGQZfz3SSWviwCe7G  
mNIvp5jEkGPCGcla**



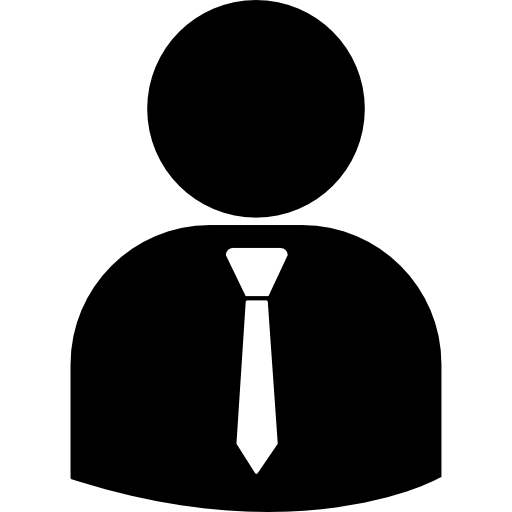
1-Sending msg

Encrypt with Key



2-Receiving msg

Decrypt By Key



4-Receiving msg

Decrypt By Key

**3- ما هي أنواع خوارزميات التشفير و ما الفرق بينها؟**

1. **Triple DES:**

* Uses three individual keys with 56 bits each. The total key length adds up to 168 bits
* Still manages to make a dependable **hardware** encryption **solution** for financial services and other industries**.**

1. **RSA :**

* A public-key encryption algorithm
* The **standard** for encrypting data sent over the internet.
* One of the methods **used** in our PGP and GPG programs.
* An **asymmetric** algorithm due to its use of a pair of keys (You’ve got your public key "encrypt" and a private key to decrypt it)

1. **Blowfish:**

* Splits messages into blocks of 64 bits and encrypts them individually.
* known for both its tremendous **speed** and overall **effectiveness**.
* Taken full advantage of its **free** availability in the public domain.
* Found in software categories ranging from e-commerce platforms for securing payments to password management tools, where it used to protect passwords (**flexible encryption**).

1. **Twofish:**

* Keys used in this algorithm may be up to 256 bits in length and as a **symmetric** technique (one key needed).
* Regarded as one of the fastest of its kind, and ideal for use in both hardware and software environments.
* Is **freely** available to anyone who wants to use it.

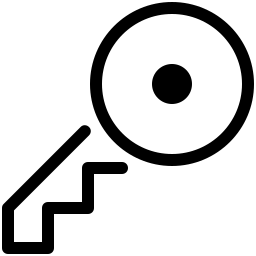
1. **AES:**

* It is extremely efficient in 128-bit form, AES also uses keys of 192 and 256 bits for heavy duty encryption purposes.
* Considered impervious to all attacks, with the exception of brute force, which attempts to decipher messages using all possible combinations in the 128, 192, or 256-bit cipher**.**

**4- بشرح مبسط و واضح اشرح كيف تعمل خوارزمية التشفير RSA (لك حرية اختيار طريقة الشرح إما بالرسم أو بالوصف).**

The figure show how public key encryption works:

Public Key: Shared with the public that wants to send data.  
Private Key: Kept secret and used only to decrypt data encrypted by our Public Key

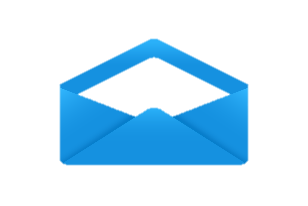


Decryption

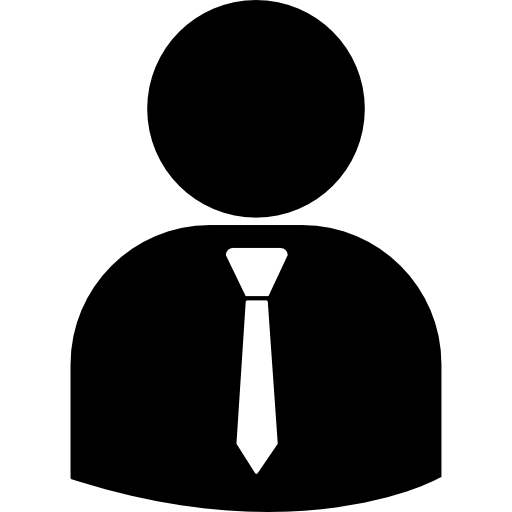
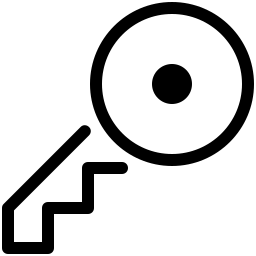
Recipient's Private Key

Encryption

Recipient's Public Key

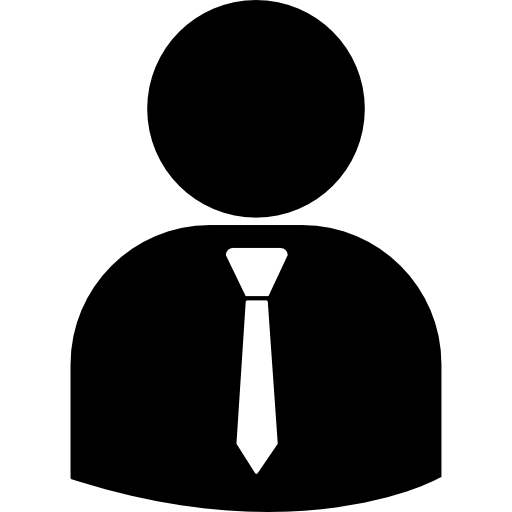


**wUwDPglyJu9LOnkBAf4vxSpQgQZltcz7LWwEquhdm5kSQIkQlZtfxtSTsmawq6gVH8SimlC3W6TDOhhL2FdgvdIC7sDv7G1Z7pCNzFLp0lgB9ACm8r5R  
N5ske9cBVjlVfgmQ9VpFzSwzLLODhCU7/2THg2iDrW3NGQZfz3SSWviwCe7G  
mNIvp5jEkGPCGcla**



Sender

Receiver



**5- تعتبر خوارزمية DES من خوارزميات Block Cipher, بشكل مبسط ما هي خوارزميات Block Cipher؟**

**A** block cipher is a deterministic algorithm operating on fixed-length groups of bits (block) with an unvarying transformation that is specified by a symmetric key.

* Operate as important elementary components in the design of many cryptographic protocols and are widely used to implement encryption of bulk data.

**6- كم عدد Bits تستخدمه خوارزمية DES وكم عدد Bits المستخدمة لأجل error detection؟**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **DES** | |  |  |  | | --- | --- | --- | | Uses three individual keys | | | | **1st 56 bits** | **2nd 56 bits** | **3rd 56 bits** | | **Total key length** = Up to 168 bits. | | | |
| **Error detection**  **“parity check”** | |  | | --- | | Even Parity Error Detection: 1’s and 0’s – 11000010, 01000011 | | Odd Parity Error Detection: 1’s and 0’s – 01000010, 11000011 | |

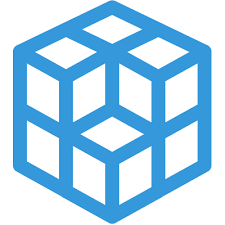
**ثانيًا: الأسئلة المتعلقة بـــ Hash Function:**

**1- ما هو سبب استخدام Hash Function ؟**

A hash function is any function that used to map data of arbitrary size onto data of a fixed size. The values returned by a hash function (hash values, hash codes, digests, or simply hashes).

* Used in combination with a hash table, a common data structure used in computer software for rapid data lookup.
* Useful in cryptography (allows one to easily verify whether some input data map onto a given hash value).

**2- بشرح مبسط و واضح اشرح كيف تعمل Hash Function (لك حرية اختيار طريقة الشرح إما بالرسم أو بالوصف).**

****

Hash Function

Math

Hash Vale

Data Block

**3- ما الفرق بين خوارزميات التشفير و Hash Function ؟ (هناك عدة أسباب، المطلوب السبب الرئيسي).**

|  |  |
| --- | --- |
| Hash Function | * An ideal way to store passwords (hashes are inherently one-way in their nature) * By storing passwords in hash format, it's very difficult for someone with access to the raw data to reverse it. * When storing a password, hash it with a salt, and then with any future login attempts, hash the password the user enters and compare it with the stored hash. |
| خوارزميات التشفير | * Encryption should only ever be used over hashing when it is a necessity to decrypt the resulting message. * If you have a use-case where you have determined that encryption is necessary, you then need to choose between symmetric and public-key encryption. |
| **If the raw value doesn't need to be known for the application to work correctly, then hashing should always be used instead, as it is more secure.** | |

**4- إقرإ عن Salt المستخدمة في Hash Function, المرجع الرابع سيوضحها لك, لأننا سنحتاجها في المهمة القادمة.**

**5- في المرجع الأخير سيكون موقع Hash Function, استكشفه.**