Quantum Computing and its Impact on Cryptography

Written by: **Kritika Roy** - July 19, 2017

https://idsa.in/backgrounder/quantum-computing-and-its-impact-on-cryptography_kroy_190717

Presented by: Juan Nicolás Sastoque Espinosa

TOPICS

- Introduction
- Birth of Modern Encryption
- Applications of Encryption
- Why the Need to Encrypt?
- Challenges to Contemporary Encryption Processes
- Where Does Encryption Stand Today?
- The Future of Encryption
- Conclusions

Introduction

The world begin to move from **classical computing** to **quantum computing** (which may have the power to break the strongest blocks)

A dilemma came to the fore, what are the options?

- maintaining an individual's right to privacy.
- state’s obligation to undertake data surveillance in the interest of security.

Introduction

Cryptography has been used since ancient times for many purposes:

- protect trade secrets
- military orders
- keep confidential information from neighbours.

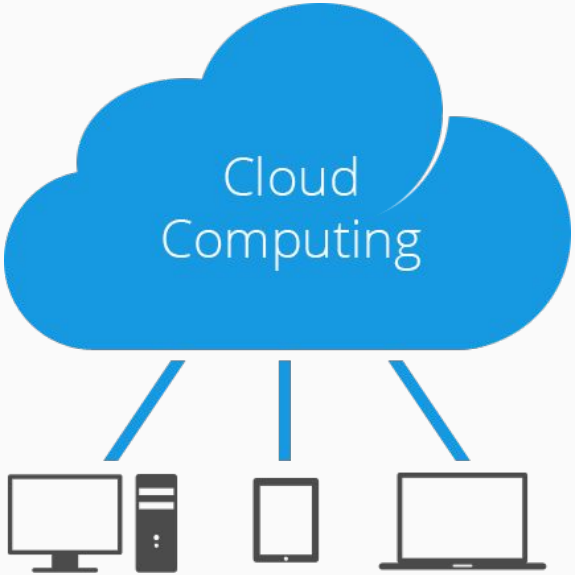
Among the methods used are:

- mask the data
- replace part of the message

Introduction

Cloud Computing allows us to access information from anywhere at any time but it brought with it certain consequences to consider:

- proliferation of high-profile data breaches
- need for more advanced encryption systems to secure confidential data

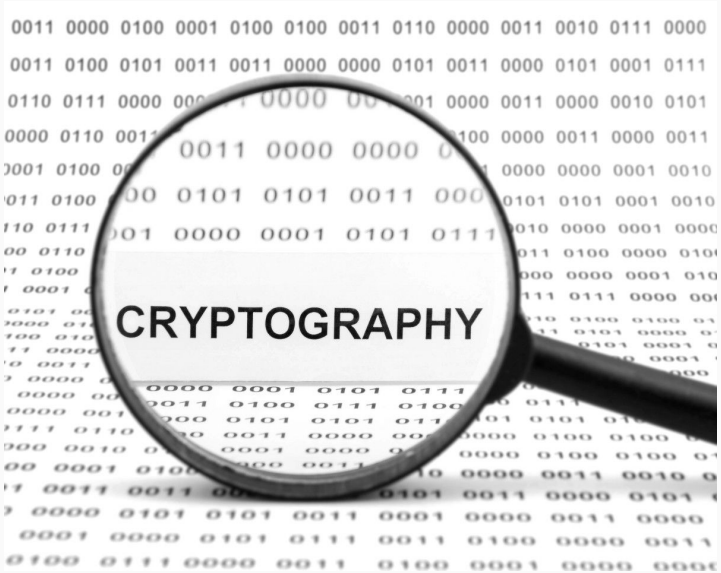


Birth of Modern Encryption

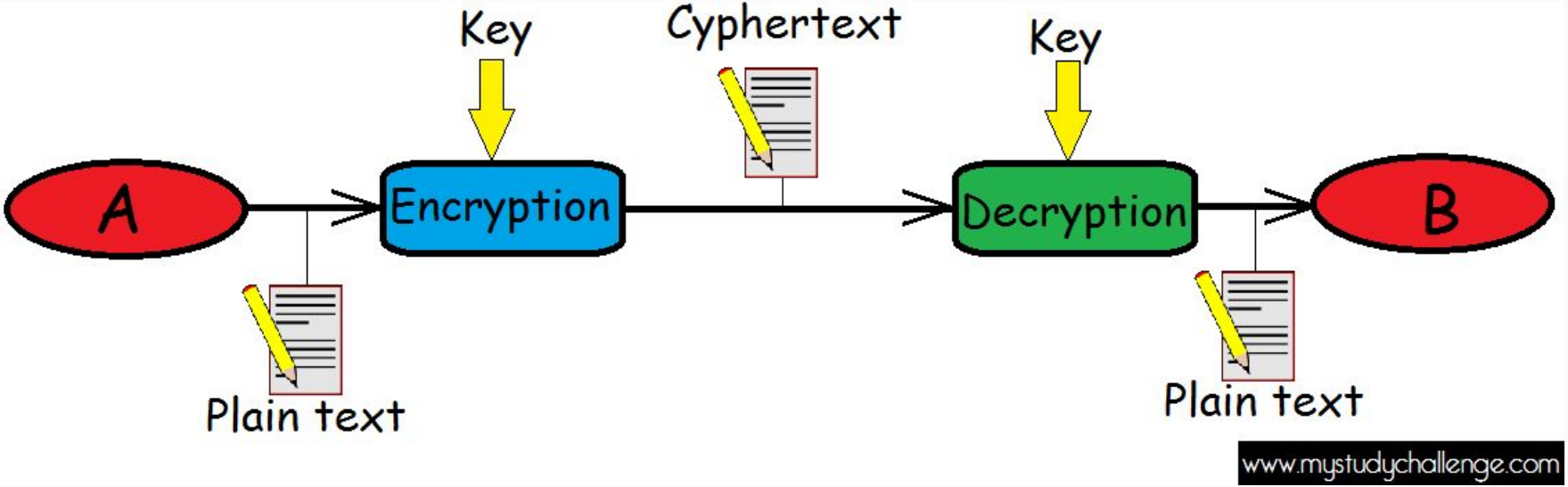
The word “**encryption**” is derived from the Greek word *kryptos*, which means “hidden”

The basic idea of encryption is to ensure confidentiality and provide security:

- authentication
- integrity
- non-repudiation



Birth of Modern Encryption



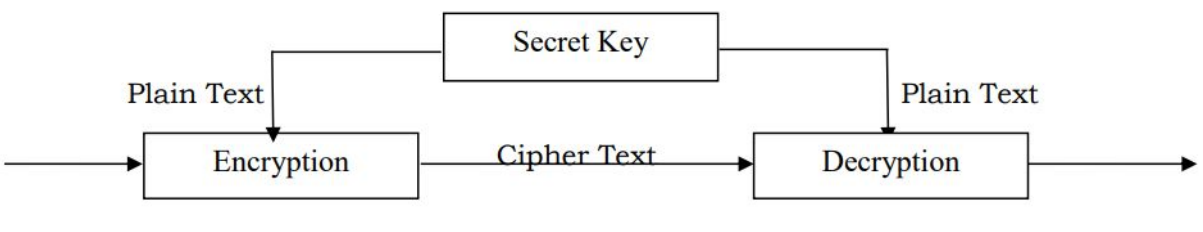
Birth of Modern Encryption

There are two main forms of encryption:

- Symmetric Key Encryption
- Public Key Encryption

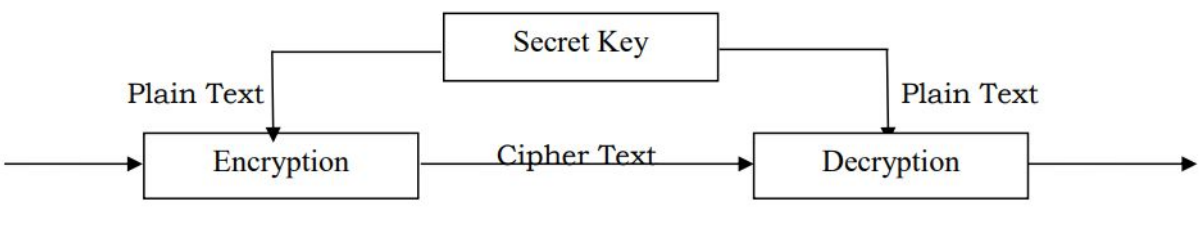
Birth of Modern Encryption

Symmetric Key Encryption



Birth of Modern Encryption

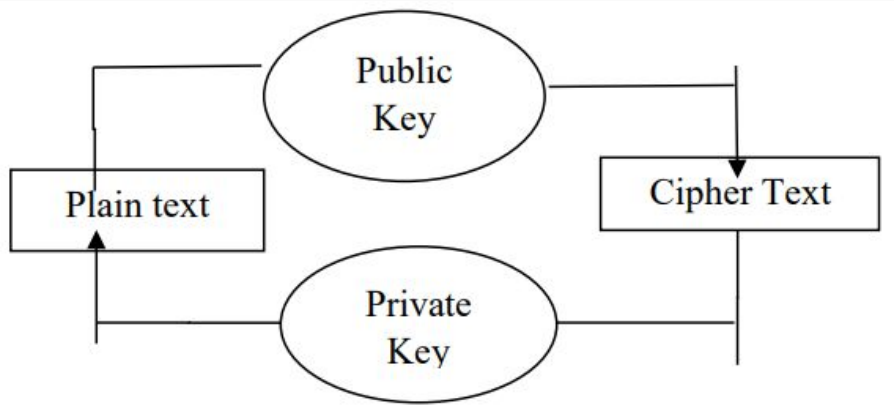
Symmetric Key Encryption



It makes use of a secret key to enable the **sender** to rearrange the data into coded form and the **recipient** to unlock the data

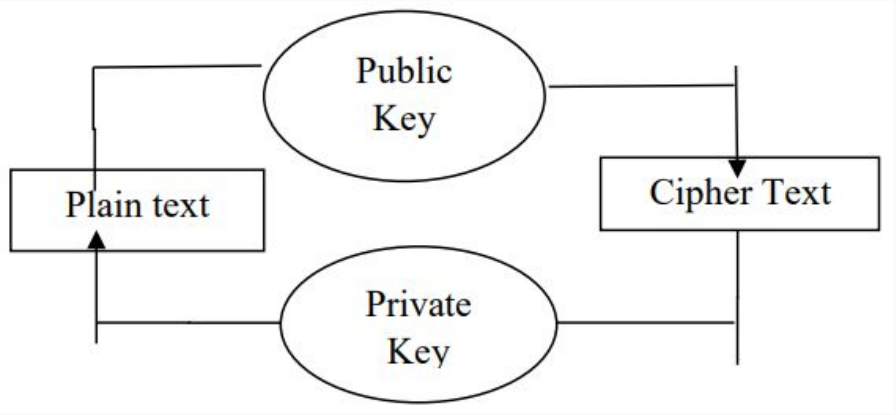
Birth of Modern Encryption

Public Key Encryption



Birth of Modern Encryption

Public Key Encryption



Was created by: ” by Whitfield Diffie, Martin Hellman, and Ralph Merkle.

uses different sets of keys for encryption and decryption – one is the private key or the secret key, while the other is a public key.

Applications of Encryption

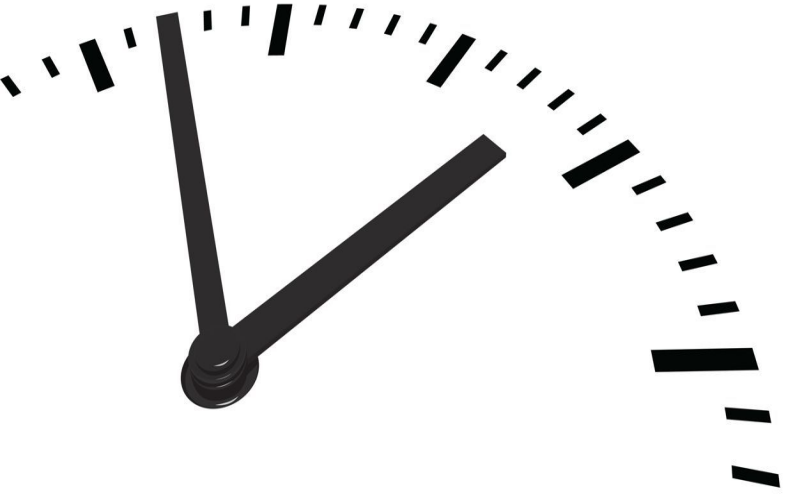
- Full Disk Encryption
- File Encryption
- End-to-end (E2E) Encryption
- Encrypted Web Connections
- Encrypted e-mail Servers

Why the Need to Encrypt?

- Encryption makes it possible to reap the benefits of the infrastructure while at the same time ensuring data protection and privacy

- Encryption also satisfies the PCI (Payment Card Industry) Data Security Standard of protecting stored data

Why the Need to Encrypt?



Encryption systems are continuously at work in nearly every dimension of modern technology,

Help us to coordinate plans or protect information from criminals, enemies, or spies, and also to validate basic, personal information and provide confidentiality and integrity to the data.

Challenges to Contemporary Encryption Processes

- Encryption does **not** make the data entirely secure but it provides an additional layer of security against data theft or compromise since criminals
- The most common form of attack is trying out random keys until the right one is found
- Other kind of attacks include **side channel attack**

Challenges to Contemporary Encryption Processes

- There is cryptanalysis in which once the flaw is located in the cipher then it can be very easily exploited.
- Encryption is susceptibility to human error.
- Advances in digital technology would be instrumental in breaking complex keys

Where Does Encryption Stand Today?

States in particular have pushed for special exceptions in order to gain access to encrypted data (“backdoors”, “master keys”)

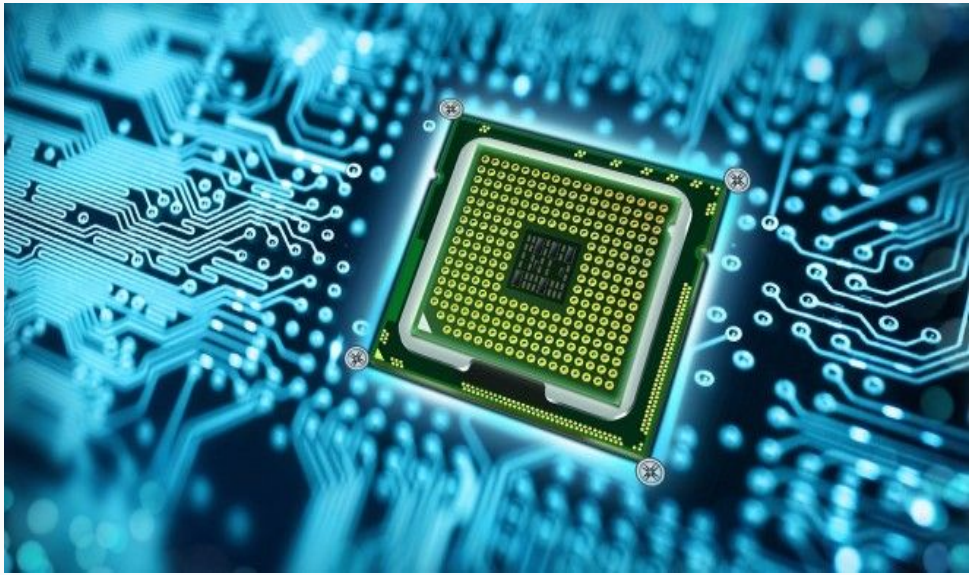
Intelligence agencies are concerned about terrorist organisations such as ISIS making effective use of social media for nefarious activities.

major private organisations handling messaging and communications services have denied such access to government agencies for carrying out unlawful eavesdropping because of business, security or technical reasons

The Future of Encryption

In 1970, there was a breakthrough in factoring called “continued fractions”

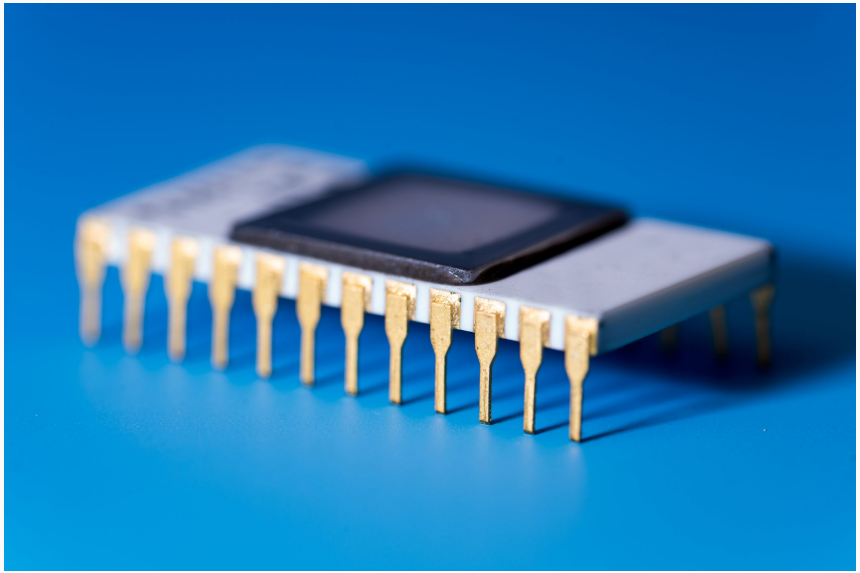
Now, with the possibility of quantum computing, which can factor large numbers in split seconds, every system that relies on encryption can easily be bypassed.



The Future of Encryption

Quantum computing commenced with the work of Paul Benioff and Yuri Manin in 1980, Richard Feynman in 1982 and David Deutsch in 1985.

Experts call the countdown as Y2Q:Y2Q: “Years to Quantum.”



The Future of Encryption

Classical computers use the binary 1-or-0 system to function.

Quantum computing uses Quantum bits or “**qubits**”. These bits are peculiar because they do not just have two states but multiple states.

The Future of Encryption

Quantum Computing might have paved the way for **Quantum encryption,** nowadays there are several scientists are in the race to deploy foolproof quantum encryption.

The unique point of using Quantum encryption is that it is impossible to interfere with messages being sent without hindering the basic properties of the message

If the message is intercepted at any given point of time, it becomes useless to the recipient.

The Future of Encryption

Quantum Encryptions also have a few stumbling blocks to overcome:

- transmission loss
- noise
- to reduce the occurrence of errors
- increase reliability across longer distances and in longer strings of information

Conclusions

Understanding Quantum technologies has become an essential national investment especially in the current medium

It becomes obligatory for states to develop and showcase “Quantum” capabilities just to have an upper hand over terrorists

True potential of Quantum computing lies in identifying all the issues that classical computers are unable to solve and then finding ways of doing so

Quantum breaking of classical encryption remains a major threat

Conclusions

If Quantum Encryption becomes a reality:

- it will not only provide secure paths for distribution of these larger keys, but also allow movement of messages in ways that cannot be intercepted

- it will have a profound and revolutionary affect on humanity

the paradoxical question of offense and defence – whether Quantum Encryption will provide unbreakable ciphers, and whether Quantum Computing will result in ciphers being cracked – remain to be answered.

UNSECURE

Nicolás Sastoque