Cryptography

Saakshi Agrawal
SY. BTECH. IT.
171081024
VJTI

12 February 2019

Guided by Pranav Nerurkar Sir
Dept. of CE & IT, VJTI, Mumbai

Contents

Introduction to Cryptography

- Cryptography or cryptology is the practice and study of techniques for secure communication in the presence of third parties.
- More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages.

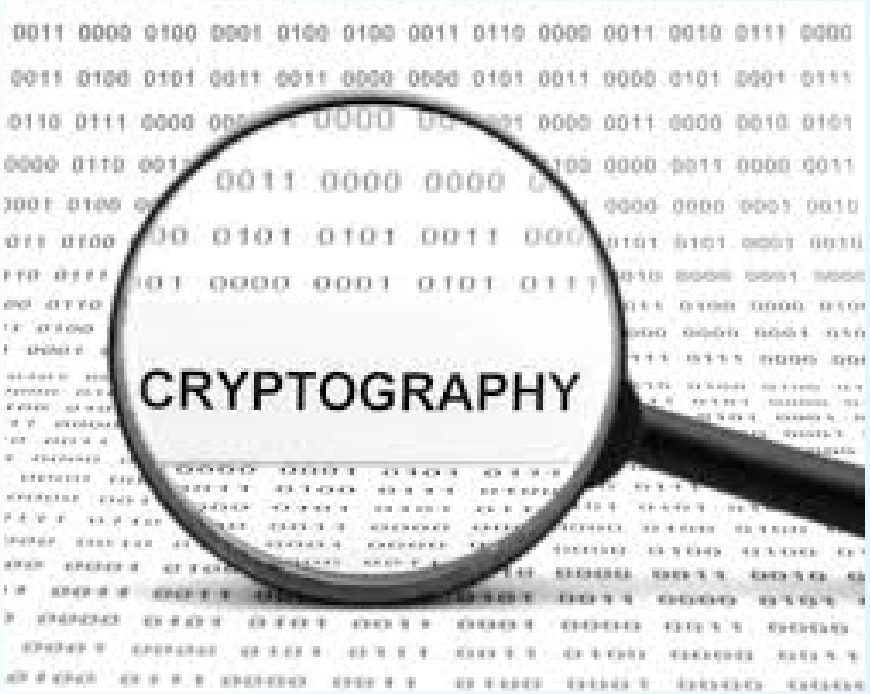

Fig 1. What is Cryptography? [1]

- Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, electrical engineering, communication science, and physics.
- Applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications.
- Until modern times, cryptography referred almost exclusively to encryption, which is the process of converting ordinary information (called plaintext) into unintelligible form (called ciphertext).
- Decryption is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext.
- A cipher (or cypher) is a pair of algorithms that create the encryption and the reversing decryption.
- The detailed operation of a cipher is controlled both by the algorithm and in each instance by a "key".
- The key is a secret (ideally known only to the communicants), usually a short string of characters, which is needed to decrypt the ciphertext.

Secret Key Cryptography

- Secret key cryptography methods employ a single key for both encryption and decryption.
- As shown in figure, the sender uses the key to encrypt the plaintext and sends the ciphertext to the receiver.
- The receiver applies the same key to decrypt the message and recover the plaintext.
- Because a single key is used for both functions, secret key cryptography is also called symmetric encryption.

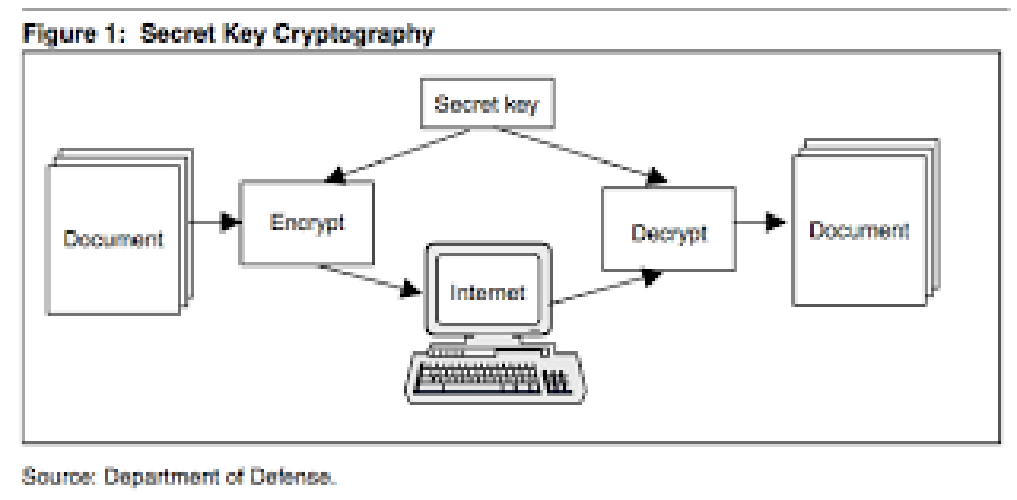

Fig 2. Secret Key Cryptography [2]

Public Key Cryptography

- Public key cryptography (PKC) is an encryption technique.
- A message sender uses a recipient's public key to encrypt a message. To decrypt the sender's message, only the recipient's private key may be used.
- The two types of PKC algorithms are RSA and Digital Signature Algorithm (DSA).

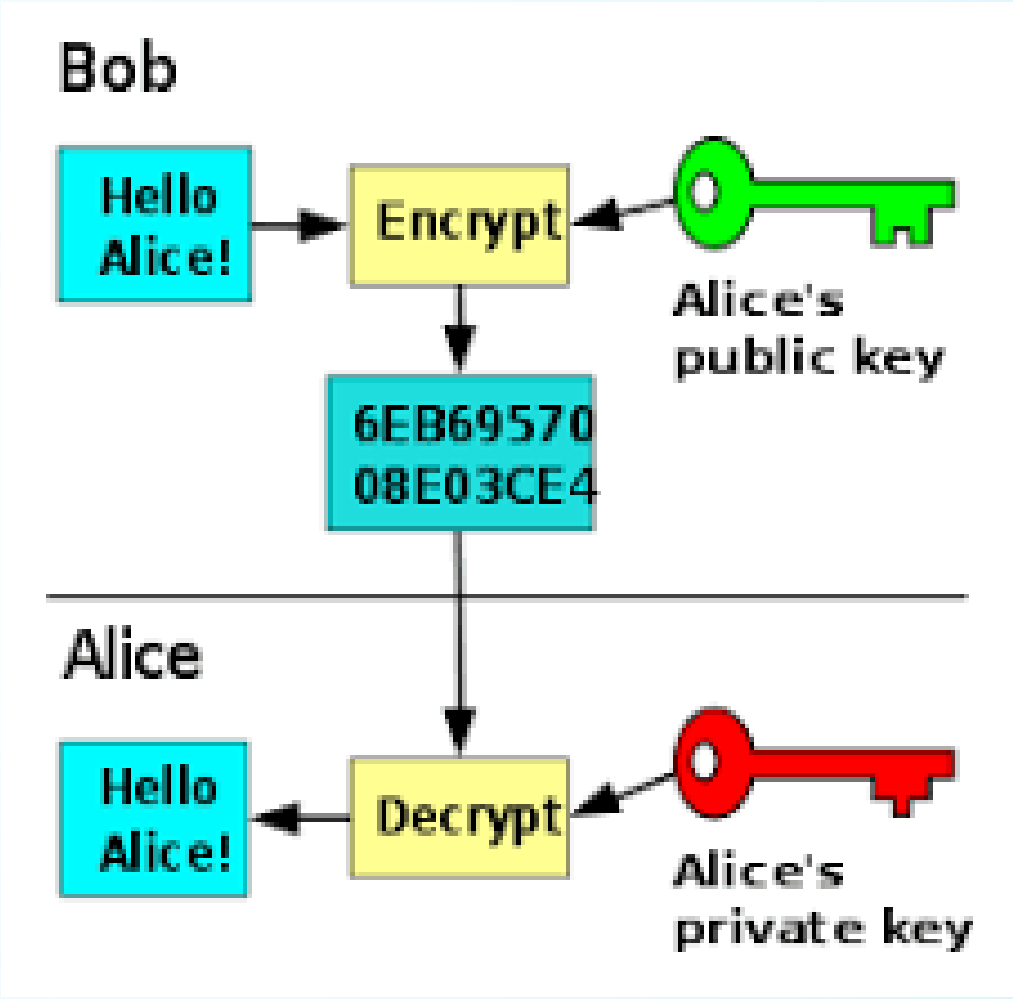

Fig 3. Public Key Cryptography [2]

Hash Functions

A hash function takes an input (or 'message') and returns a fixed-size alphanumeric string. The string is called the 'hash value'. The ideal hash function has three main properties:

1. It is extremely easy to calculate a hash for any given data.
2. It is extremely computationally difficult to calculate an alphanumeric text that has a given hash.
3. It is extremely unlikely that two slightly different messages will have the same hash.

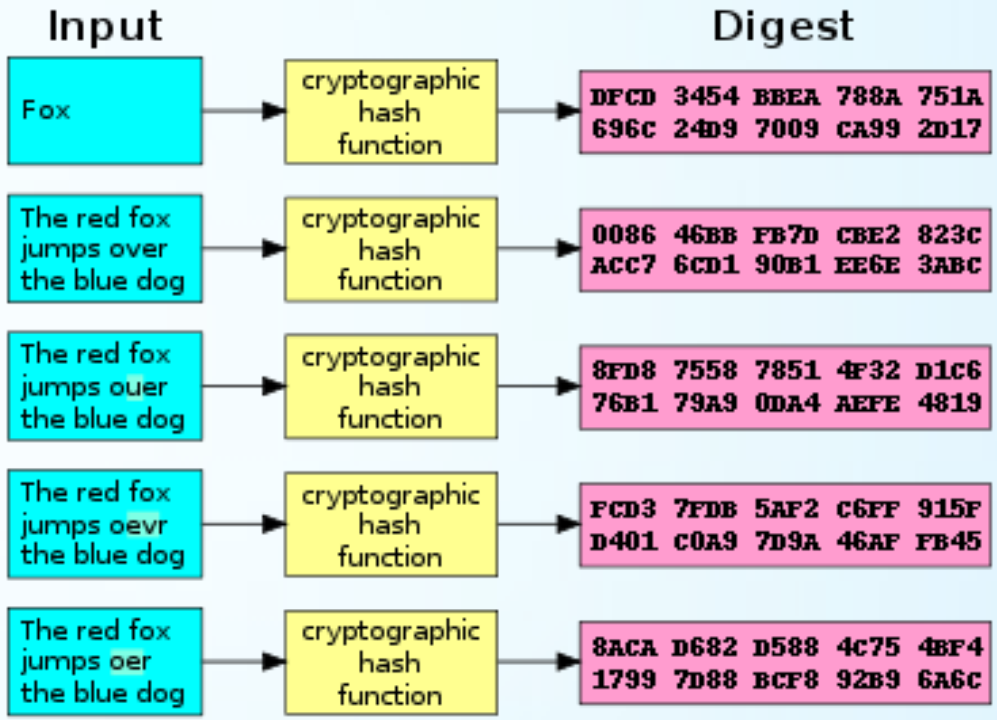

Fig 4. Hash Functions [2]

Table: Cryptography Primitives

Services	**Encryption**	**Hash Function**	**MAC**	**Digital Sign**
Confidentiality	Yes	No	No	No
Integrity	No	Sometimes	Yes	Yes
Authentication	No	No	Yes	Yes

Applications of Cryptography

- **Secrecy in Transmission:** Most current secrecy systems for transmission use a private key system for transforming transmitted information because it is the fastest method that operates with reasonable assurance and low overhead.

- **Secrecy in Storage:**
  - Secrecy in storage is usually maintained by a one-key system where the user provides the key to the computer at the beginning of a session, and system then takes care of encryption and decryption throughout the course of normal use.
  - Example, many hardware devices are available for personal computers to automatically encrypt all information stored on disk.
  - When the computer is turned on, the user must supply a key to the encryption hardware. [Katz, 2007]

- **Integrity in Transmission:**
  - A typical technique for assuring integrity is to perform a checksum of the information being transmitted and transmit the checksum in encrypted form.
  - Once the information and encrypted checksum are received, the information is again checksummed and compared to the transmitted checksum after decryption.
  - If the checksums agree, there is a high probability that the message is unaltered [Paar, 2009]
- **Authentication of Identity:**
  - In cryptography, a message authentication code (MAC), is a short piece of information used to authenticate a messagein other words, to confirm that the message came from the stated sender (its authenticity) and has not been changed.
  - The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content. [Katz, 2007]

- **Credentialing Systems:**
  - Electronic credentials are designed to allow the credence of a claim to be verified electronically.
  - Although no purely electronic credentialing systems are in widespread use at this time, many such systems are being integrated into the smart-card systems.
  - A smart-card is simply a credit-card shaped computer that performs cryptographic functions and stores secret information. [Paar, 2009]

Conclusion

- Cryptography is used to achieve few goals like Confidentiality, Data integrity, Authentication etc. of the send data.
- Now, in order to achieve these goals various cryptographic algorithms are developed by various people.
- For a very minimal amount of data those algorithms wouldnt be cost effective since those are not designed for small amount of data.
- The aim of this work was to design and implement a new algorithm to address this issue so that we dont have to apply those algorithms (which are not cost-effective) to encrypt a small amount of data.
- Algorithm has been designed in a quite simple manner but of-course not sacrificing the security issues.
- A single is used for both encryption and decryption i.e. it is fallen under secret key cryptographic algorithm.

References

Jonathan Katz (2007)

Introduction to Modern Cryptography

Christof Paar (2009)

Understanding Cryptography

Book for Students and Practitioners 12(3), 45 – 678

@article Cryptography,
url=https://www.garykessler.net/library/crypto.html,year=2006
url=https://en.wikipedia.org/wiki/Cryptography

Thank You!