Cryptographic Building Blocks

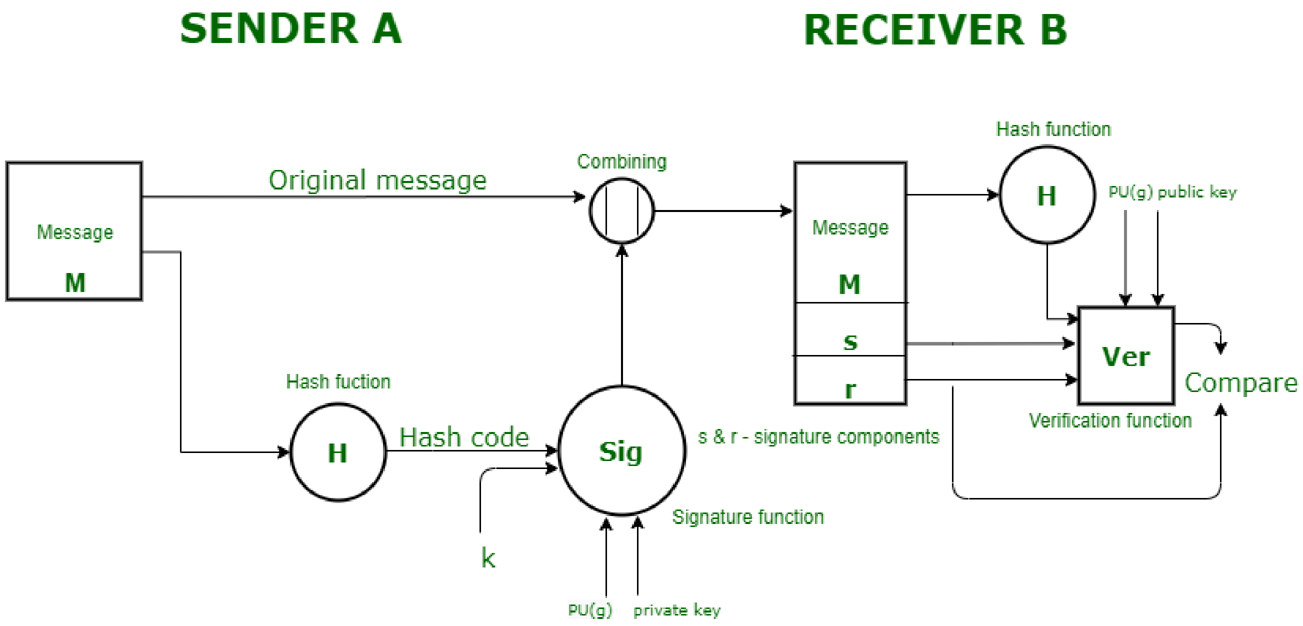
GROUP : 2

MEMBERS:

KAZI FARHAN HASAN TANJIM (18701018)
SHARIAR HASAN (18701012)
ZIHAD BEEN MOHSIN(17701009)
ROMAN MIA(18701076)
SHANTA ISLAM (17701093)
ALAMIN(17701087)
MAMUN CHOUDHURY(17701024)
ABDULLAH AL MARUF(17701075)

Digital signatures and verification using public keys

- ✓ Like electronic "fingerprints" In the form of a coded message.
- ✓ Use PKI to provide the highest levels of security and universal acceptance.
- ✓ Properties:
  - Data origin authentication
  - Non-repudiation
  - Data integrity
- ✓ Doesn't provide confidentiality.



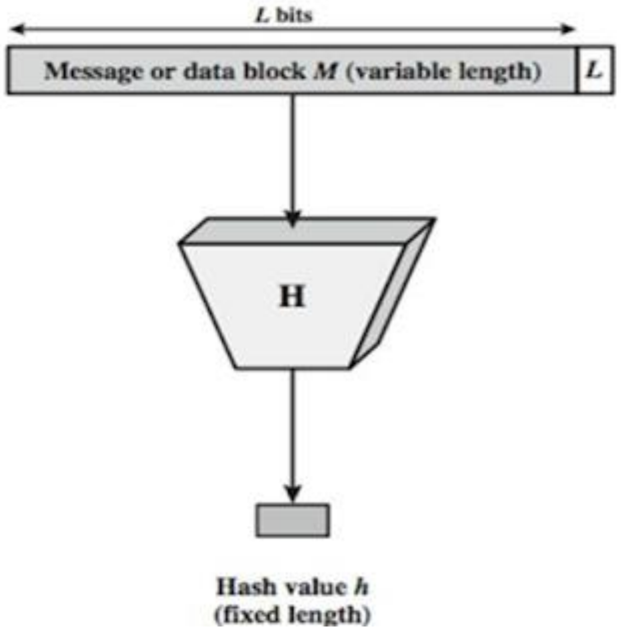
Cryptographic hash functions

- ✓ Hash function H accepts a variable length block of input data called as ‘M’ and produces the fixed size hash value can be represented as :

$$h = H(M)$$

- ✓ When hash function provides security, this is called **cryptographic hash functions**.

- ✓ Hash function protects the **integrity** of the message



Cryptographic hash functions

✓ one-way property (or preimage resistance):

- for essentially all possible hash values h, given h it should be infeasible to find any m such that H(m) = h.

✓ second-preimage resistance:

- For message m1, it means that it is difficult to produce another message m2 such that **H(m1) = H(m2).**
- i.e., it means it is infeasible to find two different messages with the same hash value.
- Its bound to a particular input m1.

✓ collision resistance:

- It means that it is difficult to find any two different messages that hash to the same value.
- i.e., it means it is hard to find m1 & m2 such that same hash value **H(m1) = H(m2).**
- Its applies to any arbitrary inputs m1, m2.

Cryptographic hash functions

✓ **Characteristics of the Hash Function**:

- Quick to calculate hash value
- (H) can be applied to variable length of data block.
- Small change in input → big change in hash value.
- One-way property , So its impossible to generate message from given hash value.
- Uses all the input data.
- Generates very different hash values for similar message.

Message Authentication

- ✓ Why Message Authentication?
  - Protecting the integrity of a message.
  - Validating identity of originator.
  - Non-repudiation of origin

- ✓ Done by data value/tag(MAC)
- ✓ Same key use for verification.

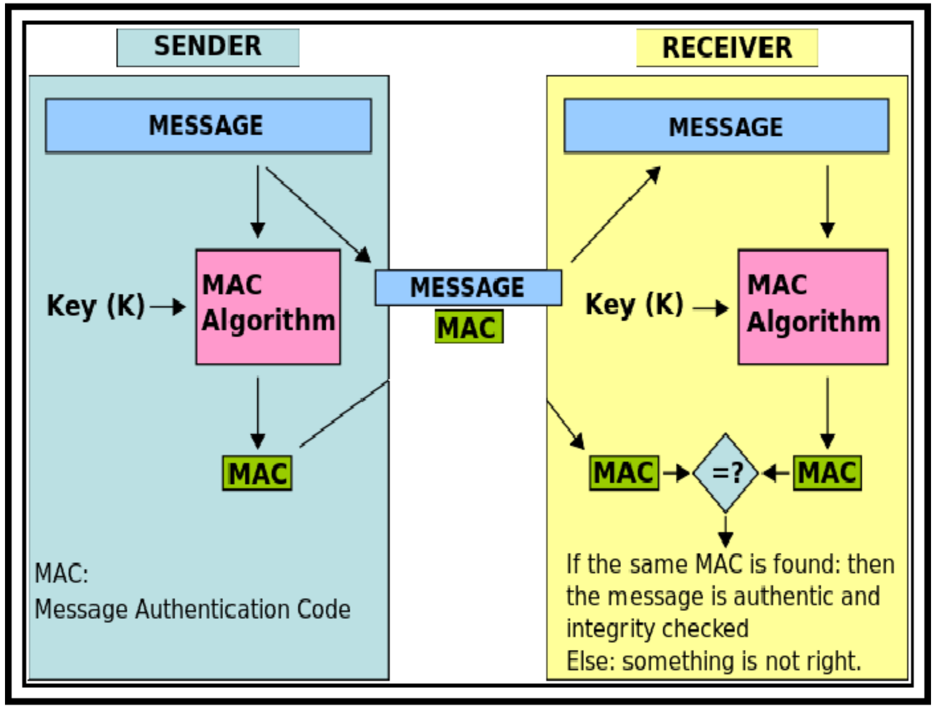
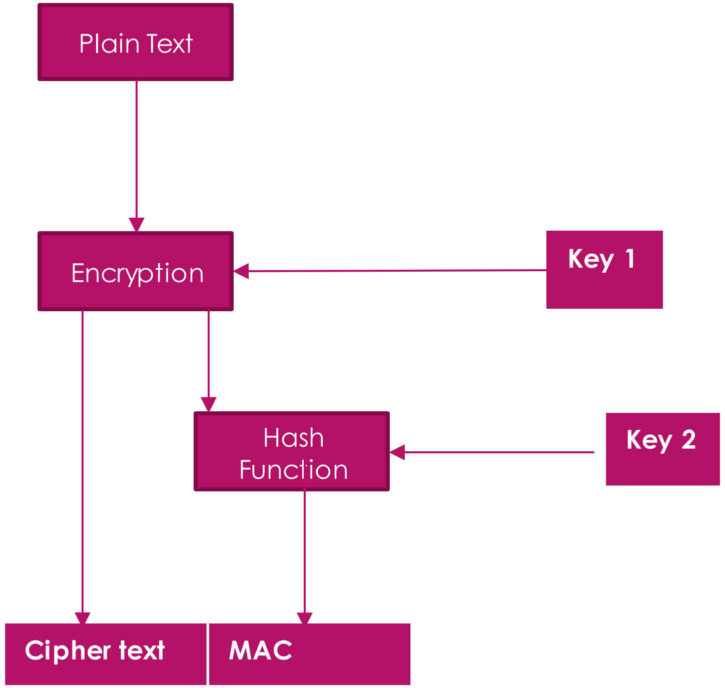

SENDER
RECEIVER
MESSAGE
MESSAGE
Key (K)
MAC Algorithm
MESSAGE
MAC
Key (K)
MAC Algorithm
MAC
MAC
=?
MAC
MAC:
Message Authentication Code
If the same MAC is found: then the message is authentic and integrity checked
Else: something is not right.

Figure 1: Working of MAC

Authenticated encryption and further modes of operation

- ✓ Authenticated Encryption(AE) can be achieved by using
  - Block cipher for encryption
  - Separate MAC algorithm for authentication
- ✓ How it works :
  - Produces an authentication tag
  - Also encrypts the message
  - Combines cipher and MAC
- ✓ Advantages :
  - Can provide security against chosen cipher attack
  - Allows detection of unauthorized cipher text manipulation
- ✓ Three approaches for operation :
  - Encrypt – then – MAC
  - Encrypt and MAC
  - MAC then encrypt



Authenticated encryption and further modes of operation

- ✓ Authenticated Encryption with Associated Data(AEAD) :
  - Same as AE
  - but need some additional information to be authenticated
  - Authenticated information can be processed before the encryption of the entire message

- ✓ Counter mode with CBC- MAC(CCM) :
  - Two pass block cipher mode
  - In essence a stream cipher with CBC-MAC for authentication

Certificates , elliptic curves and equivalent key lengths

- ✓ **Certificates:**
  - A public key certificates is a data structure.
  - It includes:

    1) A serial number to uniquely identify

    2) An expiry date

    3) Identity information for the CA.

    4) Algorithm identifiers

    5) Revocation information

- ✓ **Certification Authorities(CA):**
  - CA carries out appropriate due diligence to confirm the identity of the named subject and their association with the public key. The role of CA is critical.

Certificates , elliptic curves and equivalent key lengths

- ✓ **Certificate Revocation:**

  It allows a certificate's validity, which by default continues until the expiry date, to be terminated earlier.

- ✓ **NIST Recommended Key lengths**:

  NIST recommended at least 112 bits of security strength for symmetric key encryption and related digital signature applications.

- ✓ **Elliptic Curve Public Key System:**

  Public key functionalities can be implemented using elliptic curve.

- ✓ **Advantages:**

  Elliptic Curve Cryptography (ECC) offers computational and storage efficiencies due to smaller key size.

- ✓ **Disadvantages:**
  - It is expensive
  - It uses complex mathematics

THANK YOU