IC 3205 : Introduction to Cryptography – Part 03

Outline

- Use of encryption
- MAC
- HMAC
- Digital Signature
- Blockchain
  - NFT
- Ransomware

Three States of Data

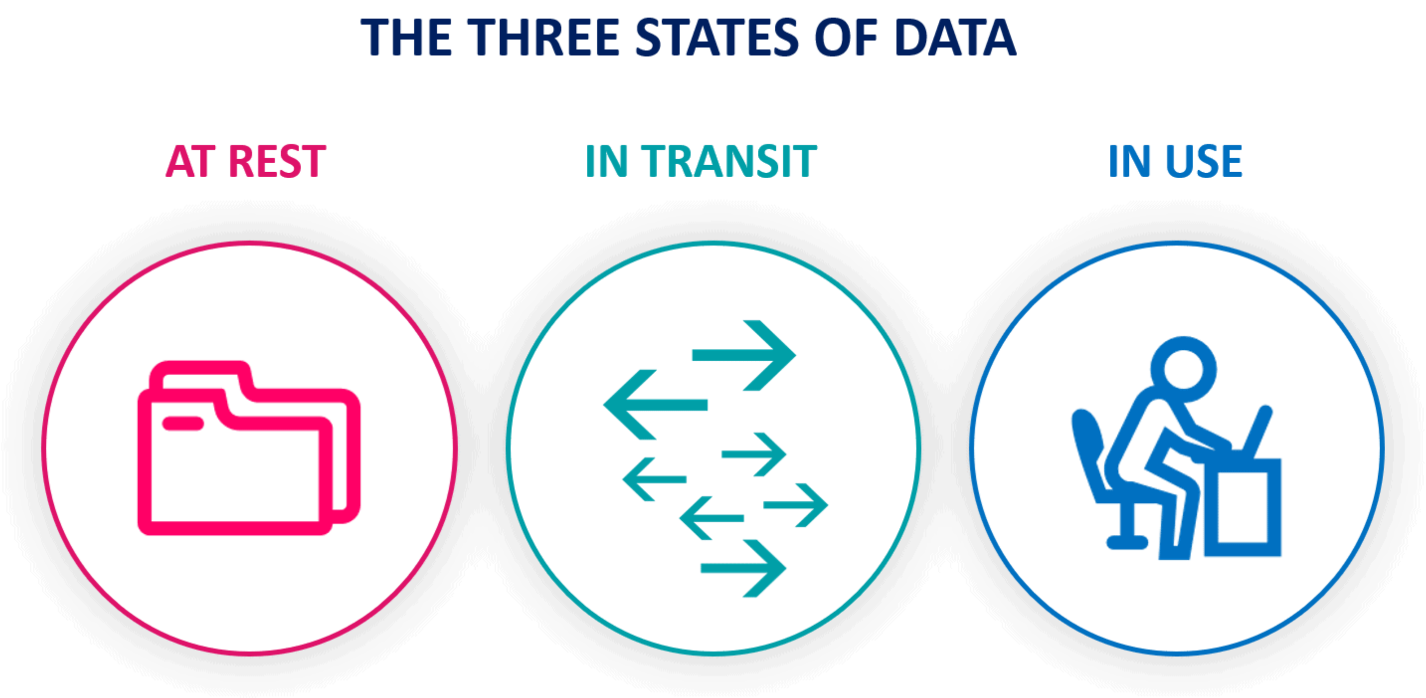


Image credit : https://images.app.goo.gl/dB49SoXfWFdoMJkS6

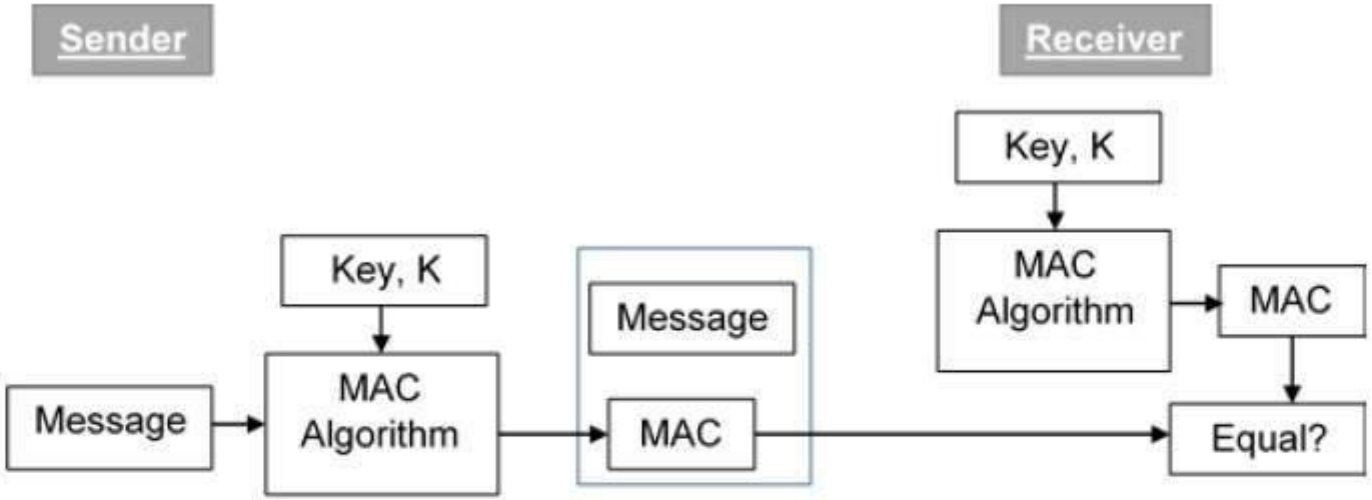
Uses of Encryption

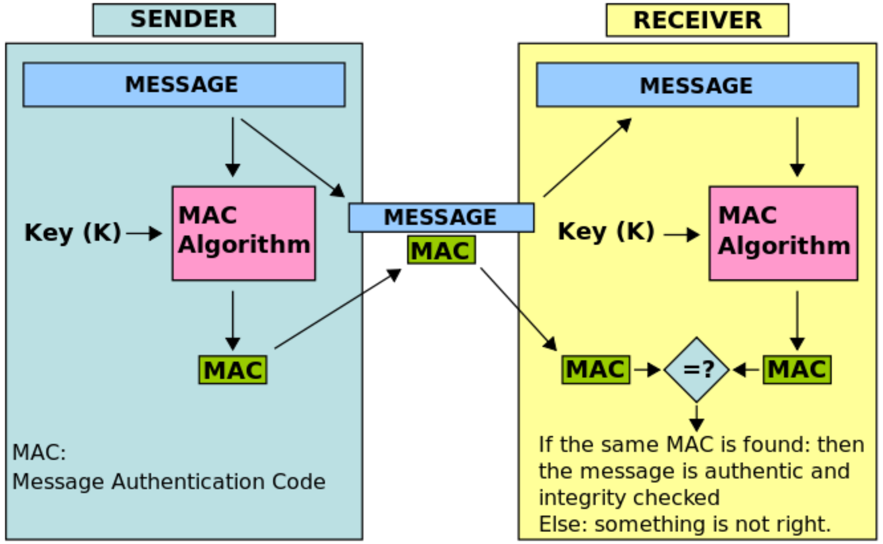
- Encryption has long been used by militaries and governments to facilitate secret communication
- It is now commonly used in protecting information within many kinds of civilian systems. (For example, the Computer Security Institute reported that in 2007, 71% of companies surveyed utilized encryption for some of their data in transit, and 53% utilized encryption for some of their data in storage
- Encryption can be used to protect data "at rest", such as files on computers and storage devices (e.g. USB flash drives)
- In recent years there have been numerous reports of confidential data such as customers' personal records being exposed through loss or theft of laptops or backup drives
- Encrypting such files at rest helps to protect them even though physical security measures fail
- Digital rights management systems **, which prevent unauthorized use or reproduction of copyrighted material and protect software against reverse engineering (see also copy protection), is another somewhat different example of using encryption on data at rest.

Message Authentication Code

- Message authentication can be provided using the cryptographic techniques that use secret keys as in the symmetric encryption
- MAC is a symmetric key cryptographic technique to provide message authentication
- For establishing MAC process, the sender and receiver share a symmetric key K
- Essentially, **a MAC is an encrypted checksum generated on the underlying message that is sent along with a original message to ensure message authentication**

Message Authentication Code (01)





MAC:
Message Authentication Code

If the same MAC is found: then the message is authentic and integrity checked
Else: something is not right.

Eg: Poly1305 MAC algorithm

Image credit : https://images.app.goo.gl/wj7SqrfzuZQK6zRA6

Message Authentication Code (02)

- Sender uses some publicly known MAC algorithm, inputs the message and the secret key K and produces a MAC value
- Similar to hash, MAC function also compresses an arbitrary long input into a fixed length output
- The sender forwards the message along with the MAC
- On receipt of the message and the MAC, the receiver feeds the received message and the shared secret key K into the MAC algorithm and re-computes the MAC value
- The receiver now checks equality of freshly computed MAC with the MAC received from the sender. If they match, then the receiver accepts the message and assures himself that the message has been sent by the intended sender
- If the computed MAC does not match the MAC sent by the sender, the receiver cannot determine whether it is the message that has been altered or it is the origin that has been falsified ; in such case can assume that the message is not the genuine.

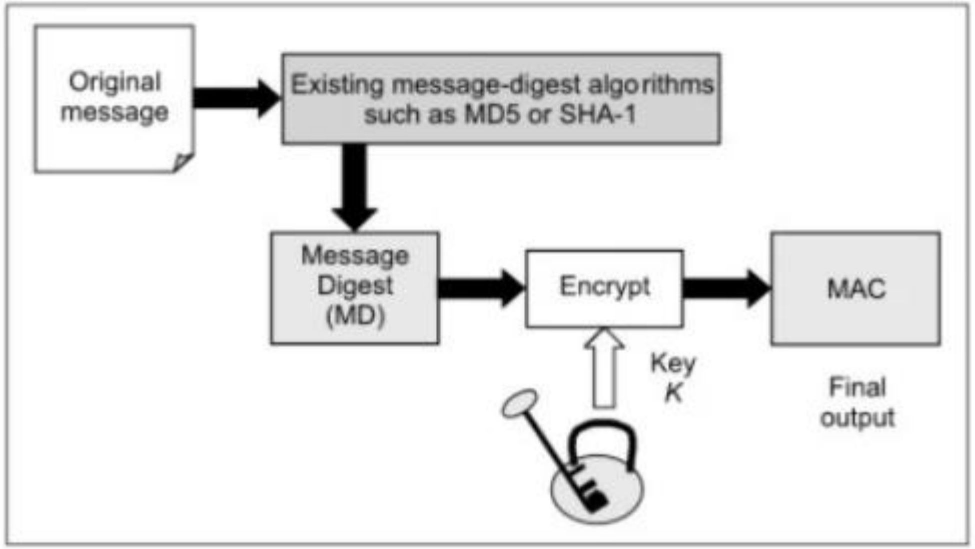
MAC Limitations

- It can provide message authentication among pre-decided legitimate users who have shared key
- This requires establishment of shared secret prior to use of MAC
- Unable to provide Non-Repudiation owing to the symmetric nature (the assurance that a message originator cannot deny any previously sent messages and commitments or actions)
- If the sender and receiver get involved in a dispute over message origination, MACs cannot provide a proof that a message was indeed sent by the sender
- Though no third party can compute the MAC, still sender could deny having sent the message and claim that the receiver forged it, as it is impossible to determine which of the two parties computed the MAC

HMAC or Keyed-Hash Message Authentication Code

- HMAC stands for Keyed-Hashing for Message Authentication
- A message authentication code obtained by running a cryptographic hash function (like MD5, SHA1, and SHA256) over the data (to be authenticated) and a shared secret key
- HMACs are almost similar to digital signatures. They both enforce integrity and authenticity
- They both use cryptography keys. And they both employ hash functions. The main difference is that digital signatures use asymmetric keys, while HMACs use symmetric keys (no public key)

HMAC


Original message
Existing message-digest algorithms such as MD5 or SHA-1
Message Digest (MD)
Encrypt
MAC
Key K
Final output

Digital Signature

- Digital signatures are the public-key version of MAC
- In real world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message
- Digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party
- Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer
- ****** In real world, the receiver of message needs assurance that the message belongs to the sender and he should not be able to repudiate the origination of that message. This requirement is very crucial in business applications, since likelihood of a dispute over exchanged data is very high ******

Digital Signature (01)

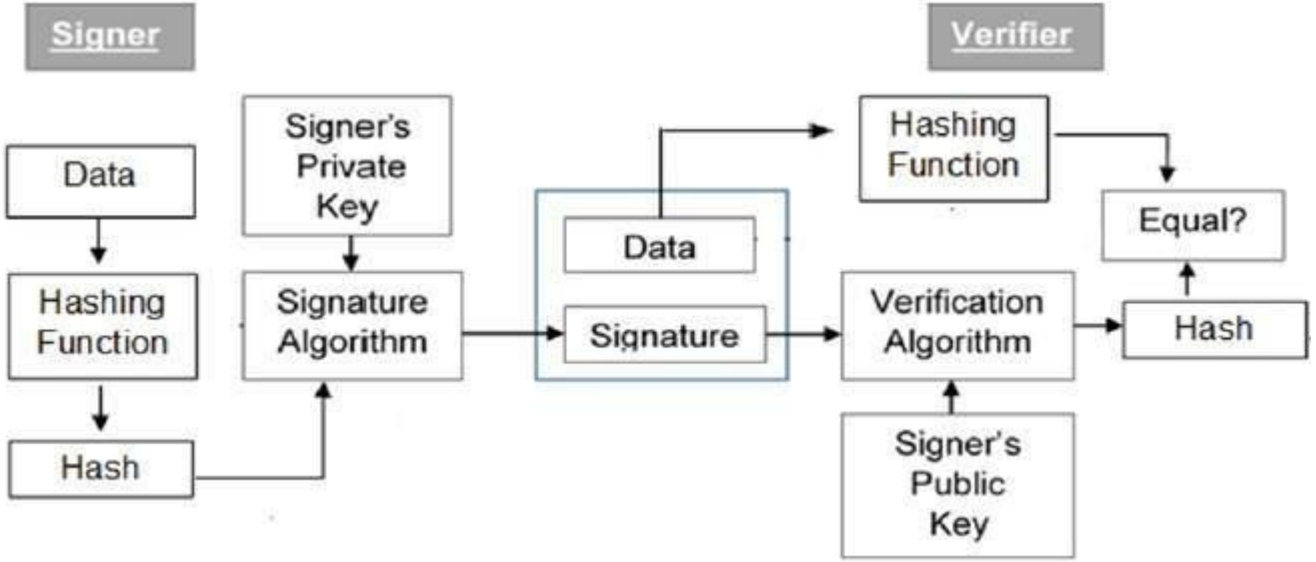


Image credit : https://images.app.goo.gl/WHwWQ9SAVcjVd4KH8

Digital Signature (02)

- The message that has to be digitally signed by signer is hashed creating a message digest (enforce data integrity)
- Hashing functions are one-way which means that the message digest cannot be reverted back to the message****
- The message digest is encrypted with signers private key ; Now this is a digital signature
- The digital signature is now attached to the original message and sent to verifier
- Once the message is received, verifier decrypts the digital signature with signers public key. This decryption results in a message digest
- Verifier also hashes the message which results in the message digest again
- If the message digests obtained near verifier are the same, then verifier can be sure that signer has signed the message and that the content of the message is as shown. Any difference in the hash values would reveal tampering of the message

Digital Signature Pros

- Message authentication : When the verifier validates the digital signature using public key of a sender, he is assured that signature has been created only by sender who possess the corresponding secret private key and no one else
- Data Integrity : In case an attacker has access to the data and modifies it, the digital signature verification at receiver end fails. The hash of modified data and the output provided by the verification algorithm will not match. Hence, receiver can safely deny the message assuming that data integrity has been breached
- Non-repudiation : Since it is assumed that only the signer has the knowledge of the signature key, he can only create unique signature on a given data. Thus the receiver can present data and the digital signature to a third party as evidence if any dispute arises in the future

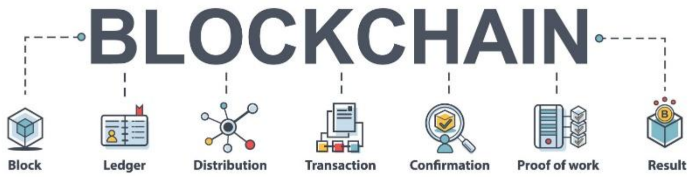


Image credit : https://images.app.goo.gl/mx7qveuVfBMNSh9n7

Trends : Blockchain

- Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system
- Is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain
- Each block in the chain contains a number of transactions
- Every time a new transaction occurs on the blockchain, a record of that transaction is added to every participant's ledger -> uses cryptographic hashing , digital signatures *****
- FYI : https://www.comparitech.com/crypto/cryptography-blockchain/
- https://medium.com/brandlitic/cryptography-in-blockchain-explained-df11fe1bd0f7

NFT

- NFT stands for "non-fungible token.“
- An NFT is basically data that is stored or accounted for in a digital ledger, and that data represents something specific
- An NFT can, for example, represent a piece of art, a music album or other types of digital files
- When you buy an NFT, you are essentially buying a digital recording of ownership of a token, which can then be transferred to a digital wallet
- The recording (or ledger) where that token is certified as proof of ownership is called a blockchain
- This is similar technology to where Bitcoin, Ethereum, Litecoin and other cryptocurrencies trade (or rather where their ownership is recorded)

Image credit : https://images.app.goo.gl/6qwcw4A9UjBsZ9WH9

Ransomware

- Modern ransomware that affected billions of users un to now , such as WannaCry, Petya, NotPetya and Locky, uses a hybrid encryption scheme, with a combination of AES and RSA encryption to secure their malware against the researchers getting encrypted files back
- 04 techniques
- Only symmetric encryption ransomware
- Client asymmetric encryption
- Server Asymmetric encryption
- Server and client asymmetric encryption + symmetric encryption

FYI
https://medium.com/@tarcisioma/ransomware-encryption-techniques-696531d07bb9
https://hackernoon.com/cryptography-malware-ransomware-36a8ae9eb0b9