UNIVERSITY OF WESTMINSTER

Applied Cryptography

6COSC019W- Cyber Security

Dr Ayman El Hajjar

February 22, 2024

School of Computer Science and Engineering
University of Westminster

OUTLINE

Modern Cryptosystems Algorithms

Data Encryption Standard (DES) and 3DES

- Data Encryption Standard (DES)
  - Developed by IBM and adopted by NIST in 1977
  - 64-bit blocks and 56-bit keys
  - Small key space makes exhaustive search attack feasible since late 90s
  - Is a symmetric encryption Algorithm
- Triple DES (3DES)
  - Nested application of DES with three different keys K_A, K_B, and K_C
  - Effective key length is 168 bits, making exhaustive search attacks unfeasible
  - $C \quad EK_C(DK_B(E_KA(P))); P \quad DK_A(E_KB(D_KC(C)))$
    - Note the Encrypt and Decrypt combination
  - Equivalent to DES when KA=KB=KC (backward compatible)

ADVANCED ENCRYPTION STANDARD (AES)

- Advanced Encryption Standard (AES)
  - Selected by NIST in 2001 through open international competition and public discussion
  - 128-bit blocks and several possible key lengths: 128, 192 and 256 bits
  - Exhaustive search attack not currently possible
  - AES-256 is the symmetric encryption algorithm of choice

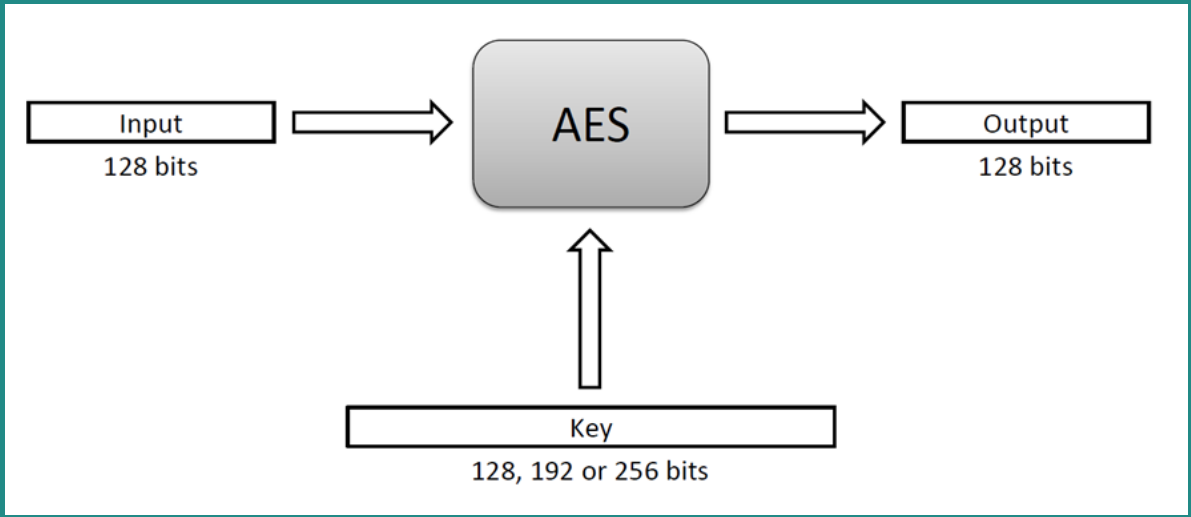


Figure 1: The Advanced Encryption Standard (AES)

ADVANCED ENCRYPTION STANDARD (AES) (CONT.)

- The 128-bit version of the AES encryption algorithm proceeds in ten rounds.
- Each round performs an invertible transformation on a 128-bit array, called state.
- The initial state X_0 is the XOR of the plaintext P with the key K:
  - $X_0 \quad PXORK$
- Round $i(i \quad 1, \ldots, 10)$ receives state Xi-1 as input and produces state X_i.
- The ciphertext C is the output of the final round: $C \quad X_10$.

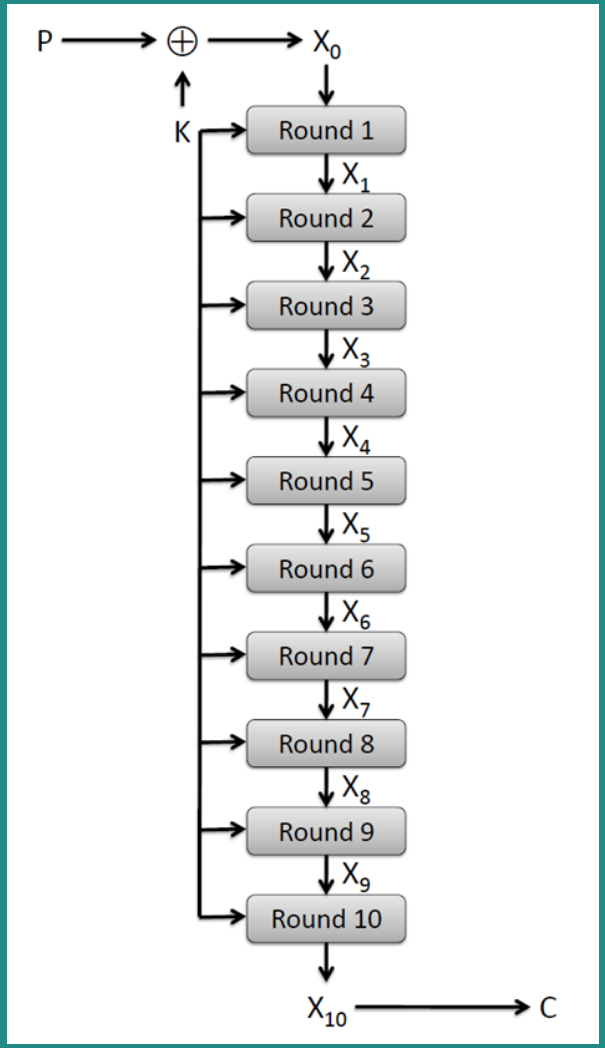
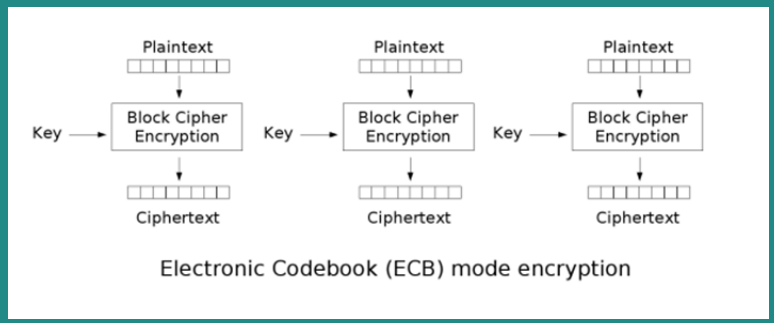


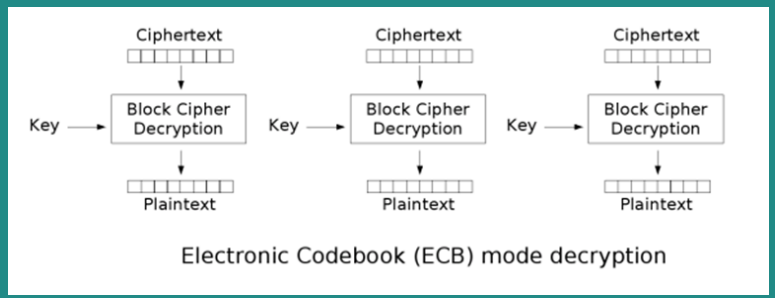
Figure 2: AES Round Structure

BLOCK CIPHER MODES

- A block cipher mode describes the way a block cipher encrypts and decrypts a sequence of message blocks.
- Electronic Code Book (ECB) Mode (is the simplest):
  - Block P[i] encrypted into ciphertext block C[i] EK(P[i])
  - Block C[i] decrypted into plaintext block M[i] DK(C[i])



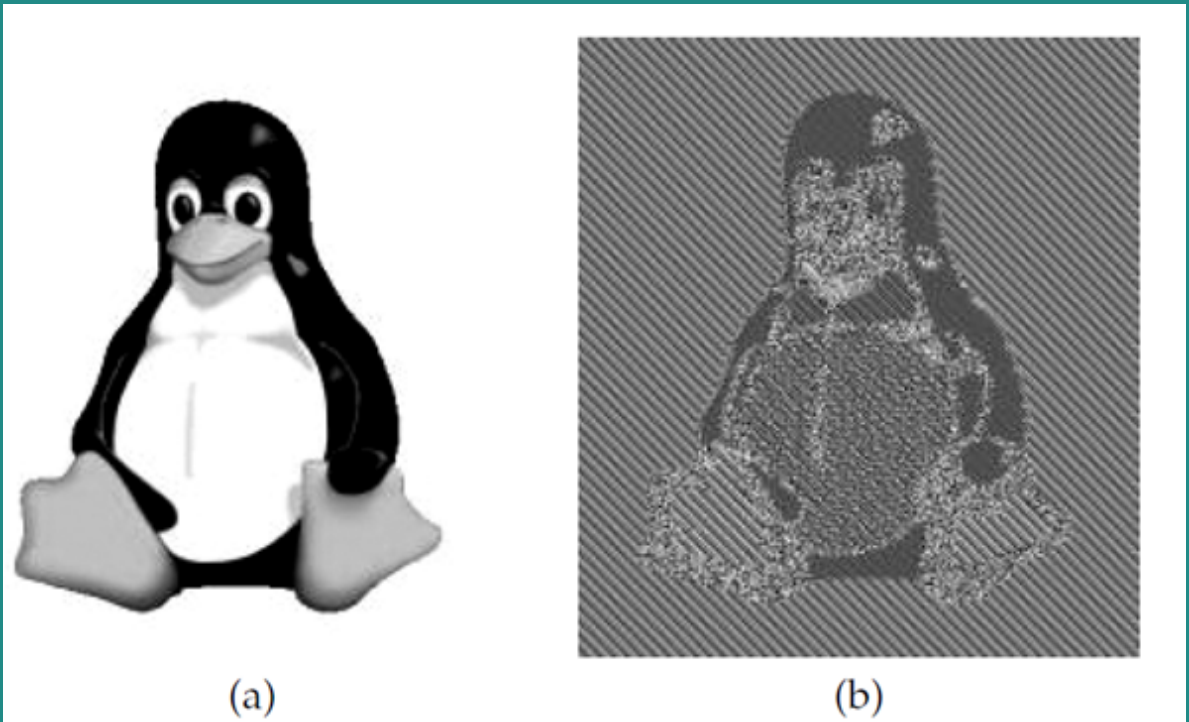
Electronic Codebook (ECB) mode encryption



Electronic Codebook (ECB) mode decryption

BLOCK CIPHER MODES

- Strengths:
  - Is very simple
  - Can tolerate the loss or damage of a block
- Weakness:
  - Documents and images are not suitable for ECB encryption since patterns in the plaintext are repeated in the ciphertext



(a) (b)

CIPHER BLOCK CHAINING (CBC) MODE

- In Cipher Block Chaining (CBC) Mode
  - The previous ciphertext block is combined with the current plaintext block $C[i]$ $EK(C[i-1] \oplus P[i])$
  - $C[-1]$ V, a random block separately transmitted encrypted (known as the initialization vector)
  - Decryption: $P[i]$ $C[i-1] \oplus DK(C[i])$
  - Is a symmetric encryption Algorithm

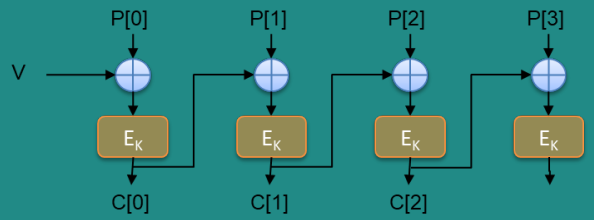


Figure 3: CBC Encryption

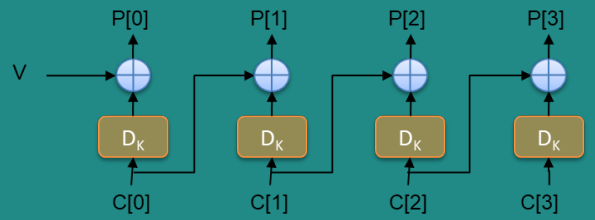


Figure 4: CBC Decryption

RIVEST CIPHER 4 (RC4)

- Designed in 1987 by Ron Rivest for RSA Security
- Trade secret until 1994
- Is a Symmetric encryption algorithm with up to 2,048 bits keys
- Simple algorithm and remarkable speed

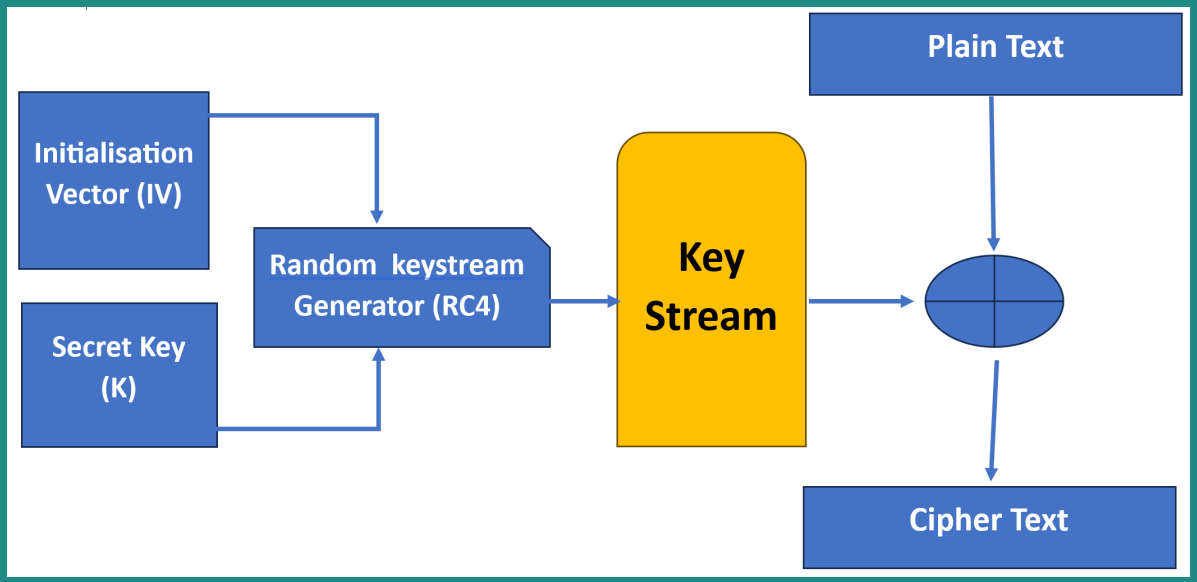


Figure 5: Rivest Cipher 4 (RC4)

ASYMMETRIC CIPHERS: RSA

- RSA (Rivest–Shamir–Adleman) is a Public key Cryptosystem that uses Block Cipher.

have a look at this example online RSA Visual

Key Generation

Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$de \bmod \phi(n) = 1$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod n$

Decryption

Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

One time Pad (OTP)

- **A one-time pad** is an extremely powerful type of substitution cipher.
- For a one-time pad encryption scheme to be considered unbreakable, each pad in the scheme must be
  - Made up of truly random values
  - Used only one time
  - Securely distributed/generated for both sides
  - Secured at sender's and receiver's sites
  - At least as long as the message

One time Pad is a form of Stream Cipher.

One time Pad (OTP) Example

Example

- Message stream 1001010111
- Keystream 0011101010
- Ciphertext stream 1010111101

To encrypt:

- The first bit of the message is XORed to the first bit of the onetime pad and so on. The result in the ciphertext value.

To decrypt:

- The receiver takes the first bit of the encrypted message and XORs it with the first bit of the pad. The receiver continues this process for the whole encrypted message, until the entire message is decrypted.

Key Management and Distribution

KEYS, KEYSPACE, AND KEY MANAGEMENT

Key

- Uses a message digest

Keyspace

- The set of all possible keys

Key management

- One of the most difficult and critical parts of a cryptosystem
- The best key management system in the world does not protect against a brilliant cryptanalyst if the encryption algorithm itself has any weaknesses

KEY DISTRIBUTION TECHNIQUES

- **Paper distribution**
  - It requires no technology to use.
  - However, it does require a person to do something to install the key.
- **Digital distribution**
  - can be in the form of CDs or email but must be protected during transmission.
  - For electronic distribution, a higher-level key, must protect the keys in transit and storage.
  - The Internet Security relies on this form of Keys distribution called public key infrastructure (PKI).
- **Hardware distribution**
  - Keys Distributed via **hardware** such as a smart card, or a plug-in module.
  - The advantage is that no copies exist outside of these components.

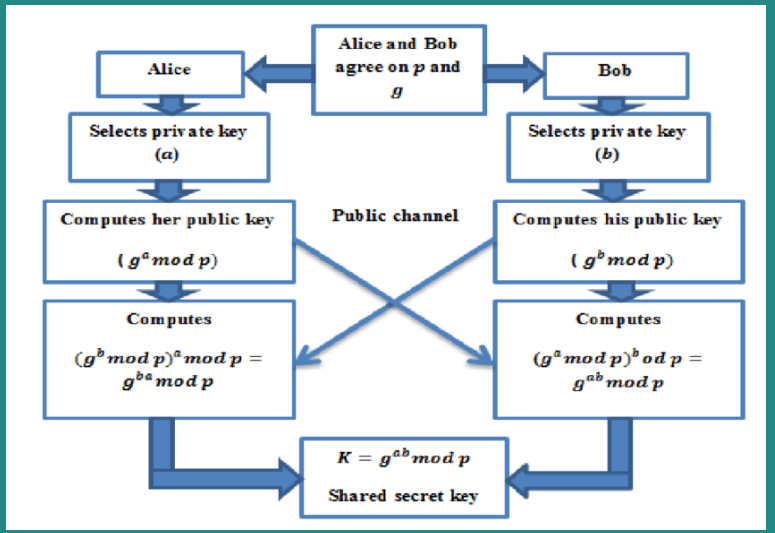
PURPOSE OF PUBLIC KEY INFRASTRUCTURE (PKI)

- Provides a mechanism through which two parties can establish a trusted relationship even if the parties have no prior knowledge of one another
- PKI brings trust, integrity, and security to electronic transactions
- PKI framework used to manage, create, store, and distribute keys and digital certificates

DIFFIE-HELLMAN KEY EXCHANGE

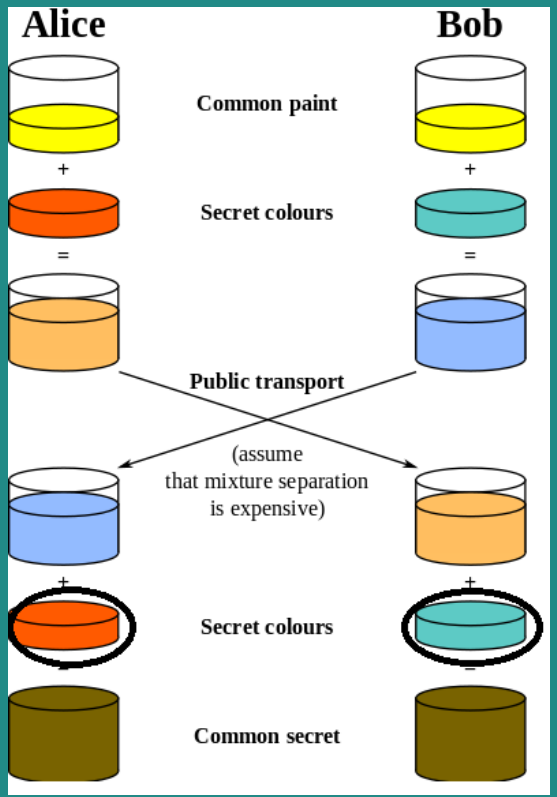
- The purpose of the algorithm is to enable two users to exchange a secret key securely that can then be used for subsequent encryption of messages.
- The algorithm itself is limited to the exchange of the keys.

1. Alice and Bob agree on a public prime number and a base.
2. Alice chooses a secret number and calculates her public value.
3. Bob chooses his secret number and calculates his public value.
4. Alice and Bob exchange their public values.
5. Each of them calculates the shared secret key using their private number and the other's public value.
6. Alice and Bob can now use this shared secret key for secure communication.



DIFFIE-HELLMAN KEY EXCHANGE EXAMPLE

1. **Common Paint**: both Alice and Bob agree on using a large prime number and a base which are public and known to everyone.
2. **Secret Colours**: Alice and Bob each choose a secret number (a private key) that they don't share with anyone.
3. **Mixing Colours**: Alice and Bob mix their secret colours with the publicly agreed colours.
4. **Creating the Shared Secret**: Using the Public Transport, Alice and Bob mix exchange their mixed colours.
5. **The common secret**: Using their previously obtained secret colours, each respectively use it with the shared secret to create the common secret.
6. Alice bob now have a common secret colour (key) that no one knows. They can use it to exchange data securely.



KEY DISTRIBUTION CENTRES /CERTIFICATE DISTRIBUTION SYSTEM

- Rather than each organization creating the infrastructure to manage its own keys, a number of hosts could agree to trust a **common key-distribution center (KDC)**
- All parties must trust the KDC
- With a KDC, each entity requires only one secret key pair—between itself and the KDC
- Kerberos use the concept of a KDC.
  - We will look at Kerberos in **Week 10- AAA and Access Control** lecture

Digital Signature and Certificates

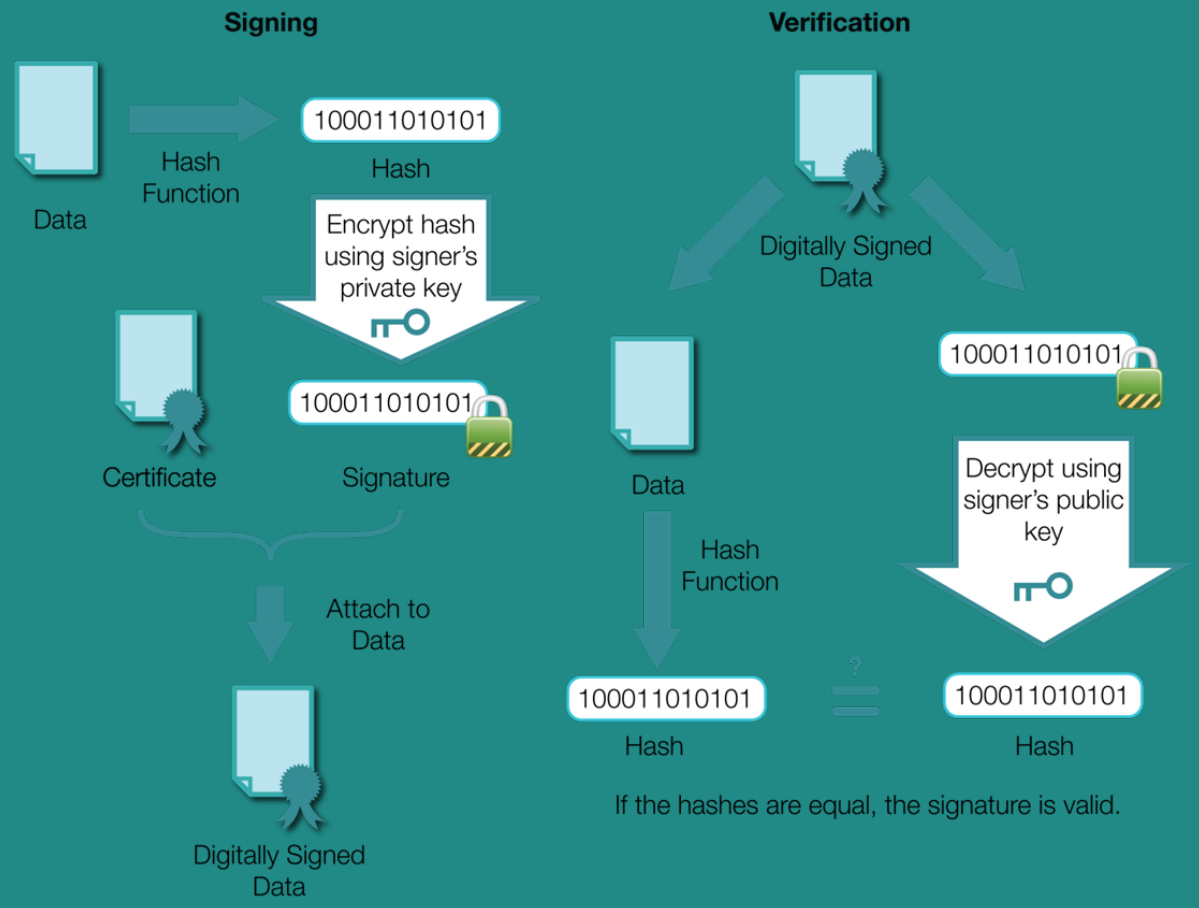
Hash and Digital Signature

- Digital signatures combine public key cryptography and hashing.
- Digital signatures (certificates) are stored in a public Key Infrastructure domain
- Creating a digital signature of existing data requires two main steps:
  1. The message or information to be sent is passed through a hashing algorithm that creates a hash to verify the integrity of the message.
  2. The hash is passed through the encryption process using the sender's private key as the key in the encryption process.
- The sender then sends the signature along with the original unencrypted message to a recipient who can reverse the process.

HASH AND DIGITAL SIGNATURE (CONT.)

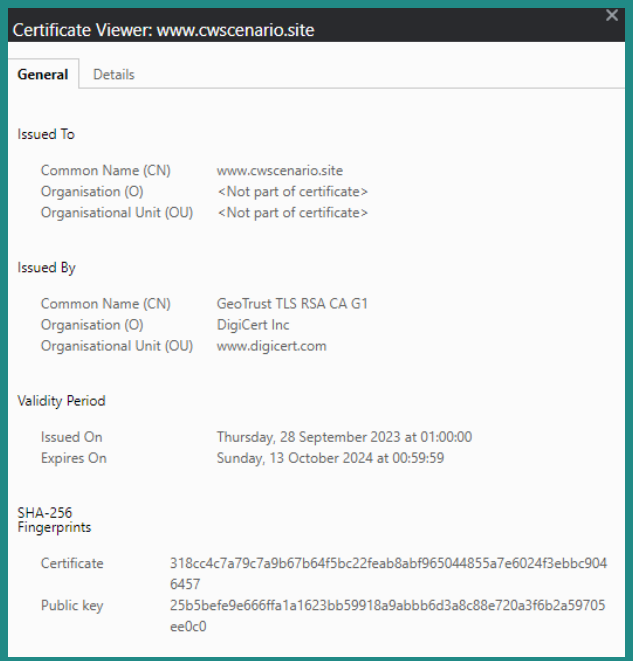
- When the receiver receives the message with the signature, that receiver will first validate the identity of the sender and then retrieve the public key to decrypt the signature.
- Once the signature is decrypted, the resulting cleartext is actually the message hash from the sender.
- Then, the receiver will run the same hashing algorithm to generate a local hash of the received message.
- Then, the hashes, both the original and the one newly created, should match.
  - If they do not, the message has been altered because the sender calculated the hash.
  - If the hash values do match, the message has been proven to come from the stated sender and has not been altered.

HASH AND DIGITAL SIGNATURE



DIGITAL CERTIFICATES

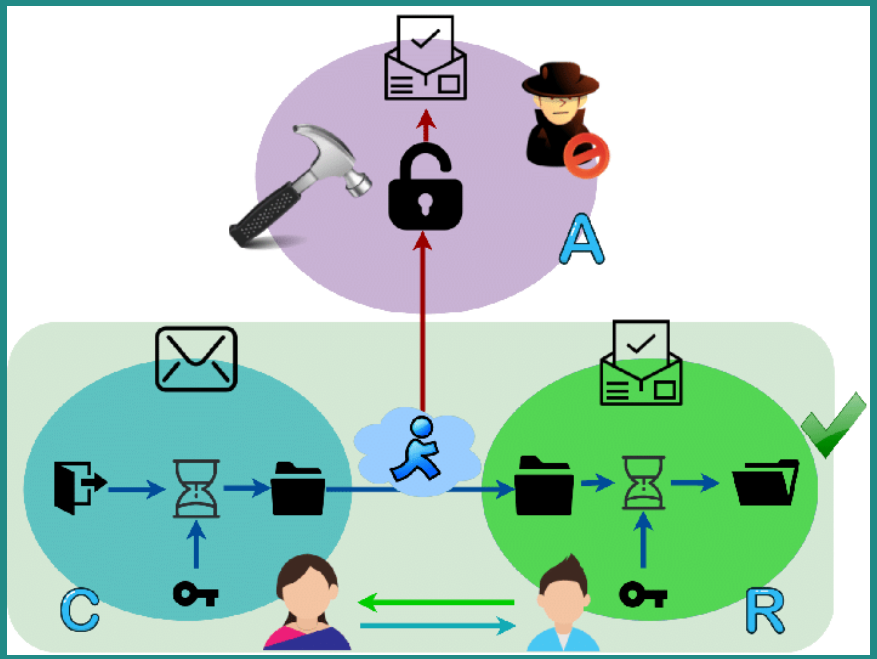
- To ensure compatibility between CAs, digital certificates are commonly built and formatted using the X.509 certificate standard.
  - X.509 certificate is used to bind the identity of owner of a public key containing information such as the public key, the hostname, the issuer, etc..



Cryptanalysis

CRYPTANALYSIS

- Cryptanalysis involves a variety of methods used by hackers and cybersecurity experts to decipher encrypted data.
  - The objective is to break cryptographic security systems and gain access to the contents of encrypted messages, without necessarily having access to the secret key used to encrypt the messages.



CRYPTANALYSIS METHODS

- **Brute Force Attack**: This method involves trying every possible key until the correct one is found. It is often time-consuming and requires significant computational power, especially against systems with long and complex keys.
- **Dictionary Attack:** This method involves the attacker using a list of common words, phrases, and previously leaked passwords to attempt to guess a password.
- **Frequency Analysis**: This technique is particularly effective against simple substitution ciphers. It involves analysing the frequency of characters or groups of characters in the ciphertext and comparing them to the expected frequencies in the language of the plaintext.
- **Known Plaintext Attack**: If the attacker has access to both the plaintext and its corresponding ciphertext, they might be able to deduce the key or identify a weakness in the encryption algorithm.

Cryptanalysis methods

- **Differential Cryptanalysis**: This method involves analysing the differences in the input that lead to differences in the output. It's often used against block ciphers to find a correlation that can help in deducing the key.
- **Rainbow Table Attack**: This method is used against hash functions and involves using precomputed tables of hash values to find plaintexts that produce certain hash values.
- **Quantum Computing**: Though still in its infancy, quantum computing poses a potential future threat to traditional cryptographic algorithms, as it could theoretically break many of the current encryption methods.

REFERENCES

- The lecture notes and contents were compiled from my own notes and from various sources.
- Figures and tables are from the recommended books
- **The lecture notes are very detailed. If you attend the lecture, you should be able to understand the topics.**
- **You can use any of the recommended readings! You do not need to read all the chapters!**
- **Recommended Readings note:** Focus on what was covered in the class.
  - Chapter 13- Cryptography, CEH v11 Certified Ethical Hacker Study Guide
  - Chapter 7, Cryptography, Fundamentals of Information Systems Security
  - Chapter 10 Cryptography & Chapter 18 Applied Cryptography, CyBOK, The Cyber Security Body of Knowledge