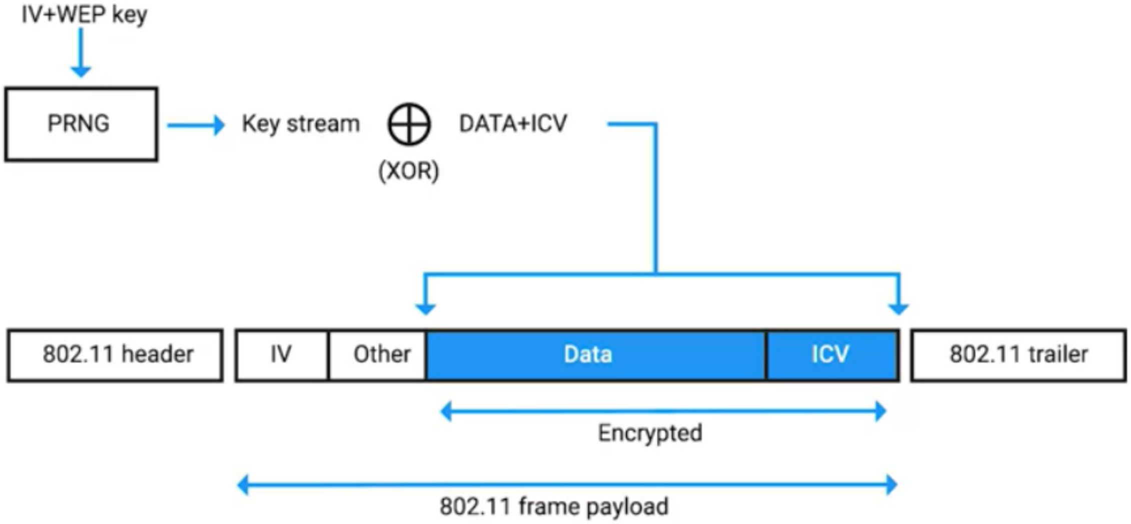
W2 Cryptography

-Aayush Tyagi

- Encryption is the act of taking a message, called plaintext, and applying an operation to it, called a cipher. So that you receive a garbled, unreadable message as the output, called ciphertext.
- The reverse process, taking the garbled output and transforming it back into the readable plain text is called decryption.
- A cipher is actually made up of two components, the encryption algorithm and the key. The encryption algorithm is the underlying logic or process that's used to convert the plaintext into ciphertext.
- Cipher Key, which introduces something unique into your cipher. Without the key, anyone using the same algorithm would be able to decode your message, and you wouldn't actually have any secrecy.
- Kerchoff's principle. This principle states that a cryptosystem, or a collection of algorithms for key generation and encryption and decryption operations that comprise a cryptographic service should remain secure, even if everything about the system is known except for the key.
- Frequency analysis is the practice of studying the frequency with which letters appear in ciphertext.
- Steganography: The practice of hiding information from observers, but not encoding it.

Symmetric Cryptography

- Symmetric-key algorithm. These types of encryption algorithms are called symmetric because they use the same key to encrypt and decrypt messages.
- A substitution cipher is an encryption mechanism that replaces parts of your plaintext with ciphertext
- A Stream cipher as the name implies, takes a stream of input and encrypts the stream one character or one digit at a time, outputting one encrypted character or digit at a time. So, there's a oneto-one relationship between data in and encrypted data out.
- block ciphers. The cipher takes data in, places that into a bucket or block of data that's a fixed size, then encodes that entire block as one unit.



-
- Now generally speaking, stream ciphers are faster and less complex to implement, but they can be less secure than block ciphers if the key generation and handling isn't done properly, if the same key is used to encrypt data two or more times, it's possible to break the cipher and to recover the plaintext. To avoid key reuse, initialization vector or IV is used. That's a bit of random data that's integrated into the encryption key and the resulting combined key is then used to encrypt the data. The idea behind this is if you have one shared master key, then generate a one-time encryption key. That encryption key is used only once by generating a new key using the master one and the IV. In order for the encrypted message to be decoded,

the IV must be sent in plaintext along with the encrypted message. A good example of this can be seen when inspecting the 802.11 frame of a WEP encrypted wireless packet. The IV is included in plaintext right before the encrypted data payload

Symmetric Encryption Algorithms

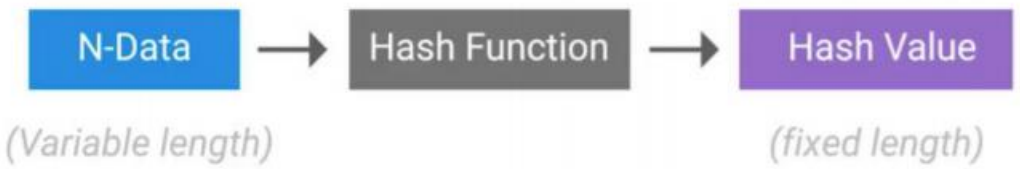
- One of the earliest encryption standards is DES, which stands for **Data Encryption Standard.** DES was designed in the 1970s by IBM, with some input from the US National Security Agency. DES was adopted as an official **FIPS, Federal Information Processing** Standard for the US. This means that DES was adopted as a federal standard for encrypting and securing government data.
- DES is a symmetric block cipher that uses 64-bit key sizes and operates on blocks 64-bits in size. Though the key size is technically 64-bits in length, 8-bits are used only for parity checking, a simple form of error checking. This means that real world key length for DES is only 56-bits.
- The NIST, **National Institute of Standards and Technology**, wanted to replace DES with a new algorithm, and in 2001, adopted **AES, Advanced Encryption Standard,** after an international competition. AES is also the first and only public cipher that's approved for use with top secret information by the United States National Security Agency. AES is also a symmetric block cipher similar to DES in which it replaced. But AES uses 128-bit blocks, twice the size of DES blocks, and supports key lengths of **128-bit, 192-bit, or 256-bit**. Because of the large key size, brute-force attacks on AES are only theoretical right now, because the computing power required (or time required using modern technology) exceeds anything feasible today.
- An important thing to keep in mind when considering various encryption algorithms is speed and ease of implementation.
- RC4, or Rivest Cipher 4, is a symmetric stream cipher that gained widespread adoption because of its simplicity and speed. RC4 supports key sizes from 40-bits to 2,048-bits

Public Key or Asymmetric Encryption
Asymmetric Cryptography

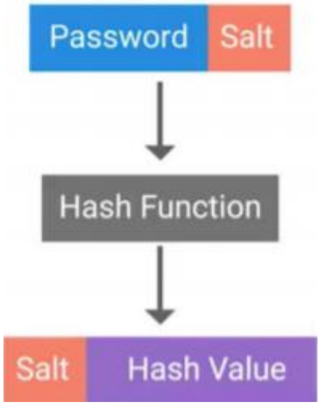
- Asymmetric encryption systems as the name implies, different keys are used to encrypt and decrypt.
- The three concepts that an asymmetric cryptosystem grants us are confidentiality, authenticity, and non-repudiation.
  (1) Confidentiality is granted through the encryption-decryption mechanism. Since our encrypted data is kept confidential and secret from unauthorized third parties.
  (2) Authenticity is granted by the digital signature mechanism, as the message can be authenticated or verified that it wasn't tampered with.
  (3) Non-repudiation means that the author of the message isn't able to dispute the origin of the message. In other words, this allows us to ensure that the message came from the person claiming to be the author
- A MAC, Message Authentication Codes, is a bit of information that allows authentication of a received message, ensuring that the message came from the alleged sender and not a third party masquerading as them.
- HMAC uses a cryptographic hash function along with a secret key to generate a MAC. Any cryptographic hash functions can be used like Shahwan or MD5 and the strength or security of the MAC is dependent upon the underlying security of the cryptographic hash function used.
- There are also MACs based on symmetric encryption ciphers, either block or stream like DES or AES, which are called CMACs or Cipher-Based Message Authentication Codes. The process is similar to HMAC, but instead of using a hashing function to produce a digest, a symmetric cipher with a shared keys used to encrypt the message and the resulting output is used as the MAC. A specific and popular example of a CMAC though slightly different is CBC-MAC or Cipher Block Chaining Message Authentication Codes. CBC-MAC is a mechanism for building MACs using block ciphers.
- **Elliptic curve cryptography or** ECC is a public key encryption system that uses the algebraic structure of elliptic curves over finite fields to generate secure keys.
- Both Diffie-Hellman and DSA have elliptic curve variants, referred to as ECDH and ECDSA, respectively

HASHING

- Hashing or a hash function is a type of function or operation that takes in an arbitrary data input and maps it to an output of a fixed size, called a hash or a digest



- Hashing can also be used to identify duplicate data sets in databases or archives to speed up searching of tables or to remove duplicate data to save space.
- Cryptographic hashing is distinctly different from encryption because cryptographic hash functions should be one directional.
- The ideal cryptographic hash function should be deterministic, meaning that the same input value should always return the same hash value.
- Hash collisions, meaning two different inputs mapping to the same output.
- SHA-1 is part of the secure hash algorithm suite of functions, designed by the NSA and published in 1995.
- It operates a 512 bit blocks and generates 160 bit hash digest. SHA-1 is another widely used cryptographic hashing functions, used in popular protocols like TLS/SSL, PGP SSH, and IPsec. SHA-1 is also used in version control systems like Git, which uses hashes to identify revisions and ensure data integrity by detecting corruption or tampering. SHA-1 and SHA-2 were required for use in some US government cases for protection of sensitive.
- A successful brute force attack against even the most secure system imaginable is a function of attacker time and resources. If an attacker has unlimited time and or resources any system can be brute forced. Yikes. The best we can do to protect against these attacks, is to raise the bar. Make it sufficiently time and resource intensive so that it's not practically feasible in a useful time-frame or with existing technology.
- **What is a Rainbow Table?**
  - A rainbow table is a database that is used to gain authentication by cracking the password hash. It is a pre-computed dictionary of plaintext passwords and their corresponding hash values that can be used to find out what plaintext password produces a particular hash.
- A password salt is additional randomized data that's added into the hashing function to generate the hash that's unique to the password and salt combination.



Cryptography Applications:
Public Key Infrastructure

- PKI is a system that defines the creation, storage and distribution of digital certificates. A digital certificate is a file that proves that an entity owns a certain public key.
- A certificate contains information about the public key, the entity it belongs to and a digital signature from another party that has verified this information. If the signature is valid and we trust the entity that signed the certificate, then we can trust the public key to be used to securely communicate with the entity that owns it.
- SSL/TLS client certificate: As the name implies, these are certificates that are bound to clients and are used to authenticate the client to the server, allowing access control to a SSL/TLS service.
- A certificate that has no authority as a CA is referred to as an End Entity or Leaf Certificate.
-

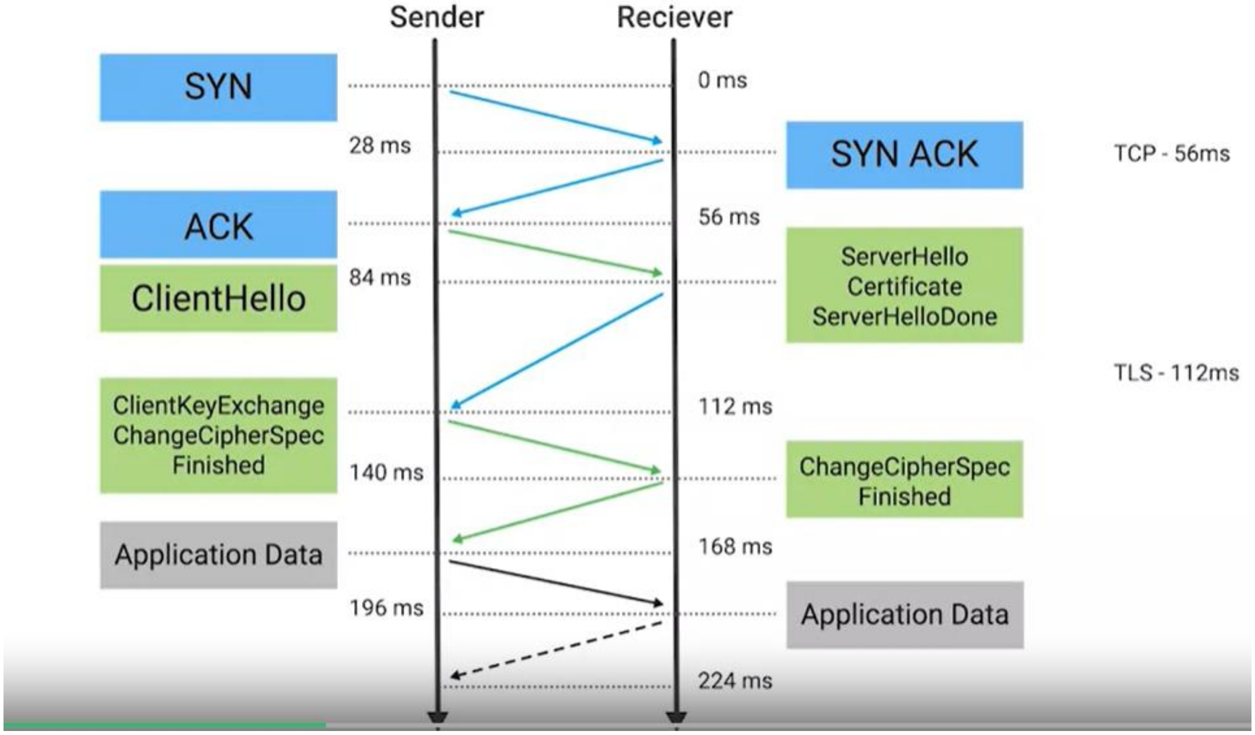
The X.509 standard is what defines the format of digital certificates.
The fields defined in X.509 certificate are, the **Version**, what version of the X.509 standard certificate adheres to.

- **Serial number**, a unique identifier for their certificate assigned by the CA which allows the CA to manage and identify individual certificates.
- **Certificate Signature Algorithm**, this field indicates what public key algorithm is used for the public key and what hashing algorithm is used to sign the certificate.
- **Issuer Name**, this field contains information about the authority that signed the certificate.
- **Validity**, this contains two subfields, Not Before and Not After, which define the dates when the certificate is valid for.
- **Subject**, this field contains identifying information about the entity the certificate was issued to.
- **Subject Public Key** Info, these two subfields define the algorithm of the public key along with the public key itself.
- **Certificate signature algorithm**, same as the Subject Public Key Info field, these two fields must match.
- **Certificate Signature Value**, the digital signature data itself.

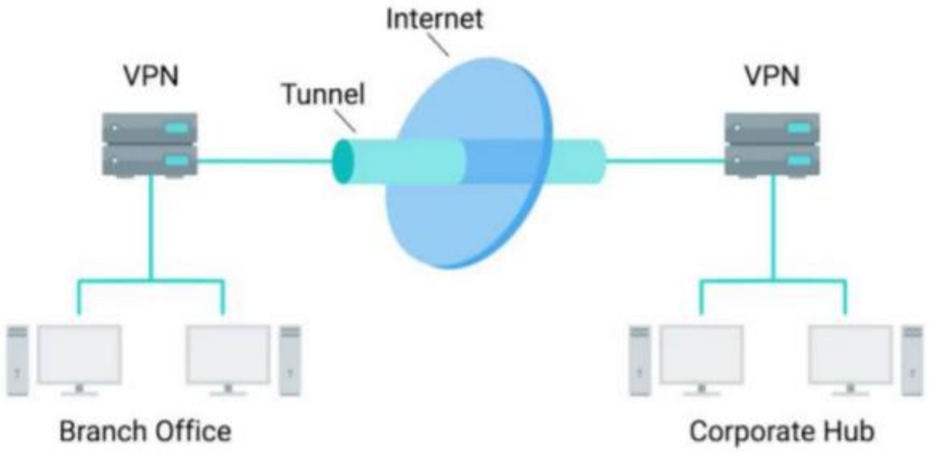
An alternative to the centralized PKI model of establishing trust and binding identities is what's called the Web of Trust. A **Web of Trust** is where individuals instead of certificate authorities sign other individuals' public keys. Before an individual signs a key, they should first verify the person's identity through an agreed upon mechanism.

Cryptography in Action

- HTTPS is the secure version of HTTP, the Hypertext Transfer Protocol.
- HTTPS can also be called HTTP over SSL or TLS since it's essentially encapsulating the HTTP traffic over an encrypted, secured channel utilizing SSL or TLS.
- TLS grants us three things.
    - One, a secure communication line, which means data being transmitted is protected from potential eavesdroppers.
    - Two, the ability to authenticate both parties communicating, though typically, only the server is authenticated by the client.
    - And three, the integrity of communications, meaning there are checks to ensure that messages aren't lost or altered in transit.
- TLS essentially provides a secure channel for an application to communicate with a service, but there must be a mechanism to establish this channel initially. This is what's referred to as a TLS handshake.



- The session key is the shared symmetric encryption key using TLS sessions to encrypt data being sent back and forth.
- Since this key is derived from the public-private key, if the private key is compromised, there's potential for an attacker to decode all previously transmitted messages that were encoded using keys derived from this private key.
- To defend against this, there's a concept of forward secrecy. This is a property of a cryptographic system so that even in the event that the private key is compromised, the session keys are still safe.
- The SSH, or secure shell, is a secure network protocol that uses encryption to allow access to a network service over unsecured networks.
- PGP stands for Pretty Good Privacy; PGP is an encryption application that allows authentication of data along with privacy from third parties relying upon asymmetric encryption to achieve this.
- A VPN is a mechanism that allows you to remotely connect a host or network to an internal private network, passing the data over a public channel, like the Internet.

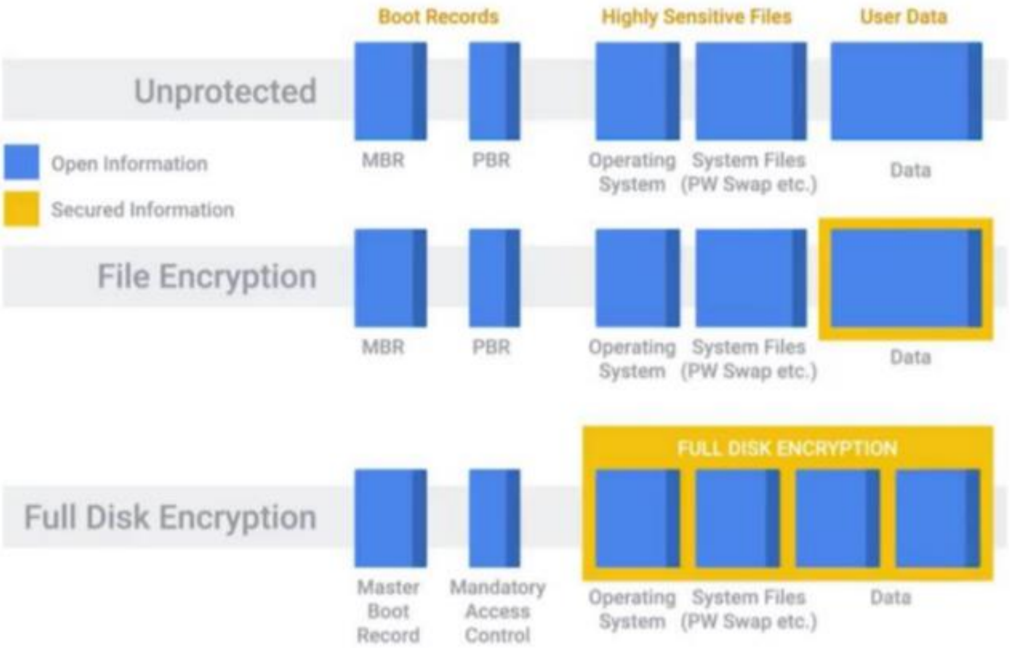


-
- IPsec, or Internet Protocol Security, is a VPN protocol that was designed in conjunction with IPv6.
- IPsec works by encrypting an IP packet and encapsulating the encrypted packet inside an IPsec packet. This encrypted packet then gets routed to the VPN endpoint where the packet is de-encapsulated and decrypted then sent to the final destination.
- IPsec supports two modes of operations, transport mode and tunnel mode.
    - When transport mode is used, only the payload of the IP packet is encrypted, leaving the IP headers untouched.
    - In tunnel mode, the entire IP packet, header, payload, and all, is encrypted and encapsulated inside a new IP packet with new headers.
- Secure communication is established using Encapsulating Security Payload. It's a part of the IPsec suite of protocols, which encapsulates IP packets, providing confidentiality, integrity, and authentication of the packets
- The tunnel is provided by L2TP, which permits the passing of unmodified packets from one network to another. The secure channel, on the other hand, is provided by IPsec, which provides confidentiality, integrity, and authentication of data being passed.
- OpenVPN can operate over either TCP or UDP, typically over port 1194

Cryptographic Hardware

- Another interesting application of cryptography concepts, is the Trusted Platform Module or TPM.
- TPM offers secure generation of keys, random number generation, remote attestation, and data binding and sealing.

Full Disk Encryption or FDE, as you might have guessed from the name, is the practice of encrypting the entire drive in the system. Not just sensitive files in the system. This allows us to protect the entire contents of the disk from data theft or tampering. Now, there are a bunch of options for implementing FDE.


Boot Records
Highly Sensitive Files
User Data
Unprotected
MBR
PBR
Operating System
System Files (PW Swap etc.)
Data
Open Information
Secured Information
File Encryption
MBR
PBR
Operating System
System Files (PW Swap etc.)
Data
FULL DISK ENCRYPTION
Full Disk Encryption
Master Boot Record
Mandatory Access Control
Operating System
System Files (PW Swap etc.)
Data