Cryptography

Is the practice and study of techniques for securing communication and data in the presence of adversaries. It involves creating written or generated odes that allow information to be kept secret.

Focus in confidentiality + integrity (hash)

Algorithms -> Methods or procedures used to encrypt and decrypt data, also defines how the encryption and decryption processes are to be carried out

Key -> Used by the cryptographic algorithms to transform the data, it is what makes your encrypted data unique

Symmetric Encryption -> Faster than asymmetric used for VPNs, Wireless Networks, files and databases, the security depend on the key length, not recommended to large companies
Symmetric Algorithms -> Use the same key for both encryption and decryption
N(N-1)/2 -> math formula to get the keys you need depend on the number of the people

Asymmetric Encryption -> Get you a digital signature because it is unique
Asymmetric Algorithms -> Public key cryptography, system that uses pairs of keys: a public key (shared with anyone) and a private key (kept with the owner)
If the public key encrypts the private decrypt (make sure the data was receive by you)
If the private key encrypts the public decrypt (make sure the data was sent by you)

Trusted Platform Module (TPM) -> Provide a hardware-based (laptops and computers) root of trust for a system, ensuring hardware-level security for encryption and authentication processes ensuring the integrity of the boot process in computing devices by verifying the integrity of the firmware and boot components.
Secure enclave -> Secure environment for sensitive operations like mobile payments

Key management system (KMS) -> Key management for encryption and decryption tasks. It does not handle certificate issuance or management
Hardware security module (HSM) -> It is like KMS but with physical separation (most used in large scale servers than TPM)
Key escrow -> Secure storage mechanism where cryptographic keys are held to ensure they can be recovered if lost

Key stretching -> technique that slow down the hashing process by repeatedly applying a cryptographic hash function to a password or key. Making it more difficult for attackers to perform brute-force attacks.

- HSM -> Physical device that manage digital keys for strong authentication
- TPM -> A specialized CHIP on an endpoint device that stores RSA encryption keys specific to the host system for hardware authentication
- EFS -> Windows Feature for individual files
- SED -> Storage drives that automatically and continuously encrypt the data on the drive without any user interaction
- FDE -> Full Disk Encryption
- BitLocker -> Windows Feature for full disk
- GPG -> FREE program used to encrypt and decrypt data, messages, and emails
- PGP -> PAID program used to encrypt and decrypt data, messages, and emails
- STARTTLS -> Upgrade the unsecure connection to TLS/SSL
- SMTPS -> OBSOLETE OF SSL/TLS
- SRTP -> Encryption for VOIP
- SHTTP -> Secure Hypertext Transfer Protocol it is the obsolete version of HTTPS