**Module 20: Cryptography**

**Concept**

* **Types:** Symmetric encryption, Asymmetric encryption
* **GAK (Government access to key)**: software companies will give **copies of all keys** (or at least a sufficient proportion of each key that the remainder could be cracked) to the government

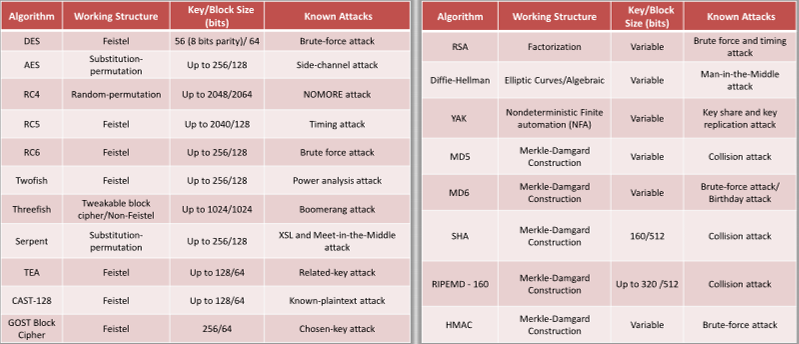
**Algorithms**

* Classic ciphers
  + substitution cipher
  + transposition cipher
* Modern ciphers:
  + Based on type of key
    - Symmetric-key algorithms
    - Asymmetric-key algorithms
  + Based on the type of input data
    - Block cipher
    - Stream cipher
* DES (Data encryption standard): blocks of **64bits data**, **56bit keys**
* AES (Advanced encryption standard)
* RC4
* RC5: 128bits
* RC6
* Twofish: 128bits, 256bits
* Threefish: 256bits, 512bits, 1024bits
* Serpent: **128 bit block**
* TEA: **Feistel cipher**, **128bits key** with **64bits blocks**
* CAST-128: 64bit block size
* DSA (Digital signature algorithm)
* RSA
* Diffie-Hellman: A cryptographic protocol that allows two parties to establish **a shared** key over an **insecure channel**, does not provide any authentication for the key exchange.
* YAK: A public-key based authenticated key exchange protocol

**Message Digest Functions**

* **MD5:** output **128 bits** fingerprint
* **MD6:** uses a Merkle tree-like structure to allow for immense parallel computation of hashes for very long inputs. It is resistant to differential cryptanalysis attacks
* **Secure Hashing Algorithm (SHA-1): 160 bits** digest
* **SHA2**: SHA256 uses **32bits** words, SHA512 uses **64bits** words
* **SHA3:** Use the **sponge construction**, in which message blocks are XORed into the initial bits of the state, which is then invertibly permuted
* **RIPEMD-160**: **RACE Integrity Primitives Evaluation Message Digest (RIPEMD)** is a **160-bit** hash algorithm
* **HMAC:** A type of **message authentication code (MAC)** that combines a cryptographic key with a cryptographic hash function. Verify the **integrity** of the data and **authentication** of a message
* **ECC (Elliptic Curve Cryptography):** A modern public-key cryptography developed to **avoid larger cryptographic key usage**
* Quantum Cryptography: Based on quantum mechanics, such as **quantum key distribution (QKD)**
* **Homomorphic Encryption:** Allows users to secure and leave their data in an encrypted format even while it is being processed or manipulated

**Comparison of Crypographic Algorithms**

* 

**Tools**

* MD5 and MD6 Hash Calculators
* HashMyFiles
* BCTextEncode

**PKI**

* A set of **hardware, software, people, policies**, and **procedures** required to create, manage, distribute, use, store, and revoke **digital certificates**
* Components:
  + **Certificate Management System:** Generates, distributes, stores, and verifies certificates
  + **Digital Certificates:** Establish people’s credentials in online transactions
  + **VA (Validation Authorizaty):** Stores certificates (with their public keys)
  + **CA (Certificate Authority):** Issues and verifies digital certificates
  + **End User**
  + **RA (Registration Authority):** Acts as the verifier for the certificate authority
* CA: Comodo, IdenTrust, GoDaddy
* Signed Certificate Vs Self-Signed Certificate
  + Signed certificate
    - User approaches a trustworthy **certification authority (CA)** and purchases a digital certificate
    - User gets the **public key** from the CA and signs the document using it
    - The signed document is delivered to the receiver
    - The receiver can verify the certificate by enquiring with **validation authority (VA)**
    - VA verifies the certificate to the receiver, but it does not **share the private key**
  + Self-signed certificate
    - User creates public and private keys using a tool, such as **Adobe Acrobat Reader, Java’s keytool, or Apple’s Keychain**
    - User uses public key to **sign the document**
    - The **self-signed document** is delivered to the receiver
    - The receiver request the **private key** from the user
    - User **shares the private key** with the receiver

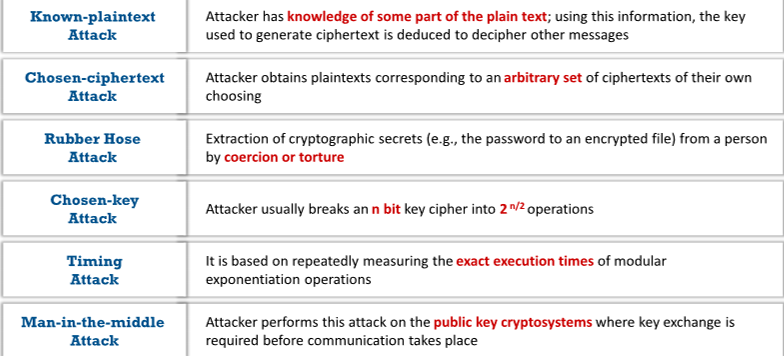
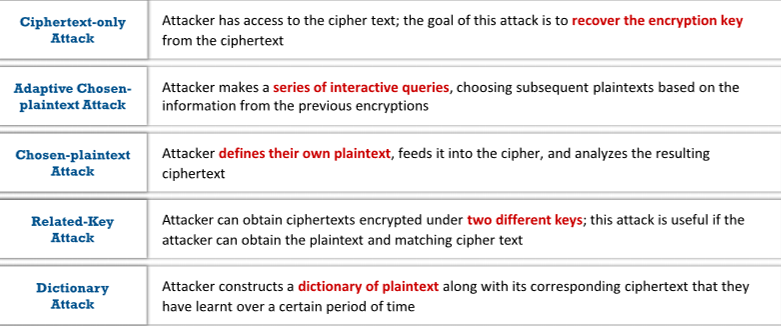
**Email Encryption**

* **Digital Signature:** Use asymmetric cryptography to simulate the security properties of a signature in digital rather than written form
* **SSL:** An application layer protocol developed by Netscape for managing the security of message transmission on the Internet. Use **RSA asymmetric (public key) encryption.**
* **TLS:** A protocol to **establish a secure connection** between a client and a server and ensure the privacy and integrity of information during transmission. Use the **RSA algorithm** with 1024-and 2048-bit strengths
* Cryptography Toolkits: **OpenSSL** is an open-source cryptography toolkit implementing **SSL v2/v3** and **TLS v1** network protocols and the related cryptography standards required by them
* **PGP (Pretty good privacy)**
  + A protocol used to encrypt and decrypt data that provides **authentication** and **cryptographic privacy**
  + Used for **data compression, digital signing, encryption** and **decryption** of **messages, emails, files, directories**, and to enhance the privacy of email communications
  + Combine the best features of both conventional and **public key cryptography** and is therefore known as a **hybrid cryptosystem**
* **GPC (GNU Privacy Guard)**:
  + A **software replacement** of PGP and free implementation of the OpenPGP standard
  + Use both symmetric key cryptography and asymmetric key cryptography
  + Use both symmetric key cryptography and asymmetric key cryptography
* **WOT (Web of Trust)**
  + **A trust model of PGP**, OpenPGP, and GnuPG systems
  + WoT is **a chain of a network** in which individuals intermediately validate each other’s certificates using their signatures
  + Every user in the network has a **ring of public keys** to encrypt the data, and they introduce many other users whom they trust
* Email Encryption Tools: **RMail**

**Disk Encryption**

* **VeraCrypt**: Establishi and maintain an **on-the-fly-encrypted** volume. On-the-fly encryption means that data is automatically encrypted immediately before it is saved and decrypted immediately after it is loaded
* **Symantec Drive Encryption:** Provide **full disk encryption** for all data
* **BitLocker Drive Encryption:** Provide offline data and operating system protection for your computer

**Cryptanalysis**

* **Linear cryptanalysis:** A known plaintect attack
* **Differential cryptanalysis**
* Integral cryptanalysis: Useful against block ciphers based on **substitution-permutation networks**, an extension of differential cryptanalysis
* **Attacks**
* **Birthday attack:** A class of brute-force attacks against cryptographic hashes that makes the brute forcing easier
* **Meet-in-the-Middle attack on Digital Signature Schemes: Encrypt from one end** and **decrypt from the other end**, thus meeting in the middle
* **Side channel attack**
* **Hash collision attack**
* **DUHK attack:** DUHK (Don't Use Hard-Coded Keys) is a cryptographic vulnerability that allows an attacker to obtain encryption keys used to secure VPNs and web sessions
* **Rainbow table attack**
* **Related-key attack: Exploite the mathematical relationship between keys** in a cipher to gain access over encryption and decryption functions
* **Padding oracle attack:** Exploit the padding validation of an encrypted message to decipher the ciphertext. Mainly performed on algorithms that operate in CBC mode
* **DROWN Attack:** a **cross-protocol weakness** that can communicate and initiate an attack on servers that support recent SSLv3/TLS protocol suites. Make the attacker **decrypt the latest TLS connection** between the victim client and server by launching malicious SSLv2 probes using the same private key.
* **Tools:** CrypTool

**Countermeasures**

* **Key strectching:** Process of strengthening a key that might be slightly too weak, usually by making it longer.
* **PBKDF2 (Password-Based Key Derivation Function 2):** A part of **PKCS #5 v. 2.01**. It applies some function (such as hash or HMAC) to the password or passphrase along with Salt to produce a derived key
* **Bcrypt:** Essentially uses a derivation of the **Blowfish algorithm**, converted to a hashing algorithm to hash a password and add Salt to it