# CompTia Notes: Cryptography

* General Cryptography Concepts
  + Substitution Cipher
    - Changing one character for another
    - “Shift all letters by 3 spaces”
  + Vigenere Table
    - Multi-alphabet substitution, secret keyword only you and the other person knows
    - Makes a graph with the alphabet on the x axis alphabet on the negative y axis
    - Find where two letters intersect (compTia and plurals, c and p, o and l, etc.)
  + Symmetric vs. Asymmetric
    - Symmetric: same key used to encrypt and decrypt
      * Key management is biggest concern
      * Key management is biggest concern, both parties must know the secret key
      * Difficult to prove identity (multiple people could know the key)
      * Faster than Asymmetric
    - Asymmetric: Has public and private key
      * Sender encrypts plain text with the recipient’s public key
      * The cipher text is sent
      * The receiver uses the private key to decrypt the cipher
      * Public and private key are mathematically linked
  + Session Keys
    - Single-se symmetric key used for encryption all communication in one communication session
    - Symmetric encryption is faster than Asymmetric
    - Asymmetric keys can be used to encrypt the session keys
  + In-band vs. Out of band key exchange
    - Out of band key exchange: Not sent over the network
      * Needs to be delivered via traditional/manual means (in-person, telephone, courier)
    - In-band key exchange
      * Done over the network as the communication session is established
      * Created in real-time then discarded once the session is over
  + Block Ciphers
    - Fixed length group of bits (blocks
    - Each block of plaintext has an equivalent size of block cipher text
  + Stream Cipher
    - Encryption takes place bit by bit using a pseudorandom cipher digit stream (keystream)
    - In a stream cipher each plaintext digit is encrypted one at a time with the corresponding digit of the keystream, to give a digit of the cipher text stream
  + Transport Encryption
    - SSL/TLS and HTTPS
    - SSL/TLS allows for secure communication over an unsecure network
    - Offers protection against eaves dropping, tampering and message forgery
    - TLS uses a handshake to check what the most secure thing each side supports and they use that
    - Only as strong as the ciphers and hashing agreed upon by both parties
    - MITM attacks exist that force both parties to agree to use unsecure protocols
    - IPsec (Internet Security Protocol)
      * Authentication header provides authentication and integrity
      * Encapsulating Secure Payload provides confidentiality along with option integrity checking
      * Adds a header, trailer, and integrity check value (ICV)
  + Non-repudiation
    - Assurance that the author of a message cannot later refute ownership
    - Asymmetric encryption functions on the premise of a secret key only the sender knows
    - Hashing: mathematical algorithm applied to a file before and after transmission
    - If anything within the file changes the hash will be completely different, then the two hashes are compared to make sure there was no change
  + Key Escrow
    - Keys needed to decrypt encrypted data are held in escrow to enable an authorized third party to access those keys
      * Referred to as a fair cryptosystem
      * Gives governments/third parties to view data if they need it
    - Recovery agents can be used to allow access to older keys
  + Steganography
    - Hiding something inside of something else
    - Mp3, image, video files can be used to hold documents
    - Image puff can be used to do this
    - Hard to detect if it is an image in another image
  + Digital Signatures
    - Signed document: document that has been hashed, and encrypted with a sender’s private key (non-repudiation)
  + Use of Proven Technologies
    - Kerckhofs’s principle states that the security of an algorithm should depend only on the secrecy of the key and not on the secrecy of the algorithm itself
    - All of the generally used encryption algorithms are publicly accessible
  + Elliptic Curve Cryptography
    - Asymmetric encryption that uses algebraic structure of elliptic curves
    - Strong encryption using smaller key size
  + Quantum Cryptography
    - Use of quantum mechanical properties to perform cryptographic tasks
    - The very act of eavesdropping disturbs the properties of the communication
    - Quantum Key Distribution (QKD)
      * Using quantum communication to establish a shared key between two parties
      * Third party (eavesdropper) can’t access or disturb the data without it being noticed
  + Ephemeral Key
    - Temp Key, used only once
    - Used to derive an additional key that is used for subsequent communication
  + Perfect Forward Secrecy
    - Session keys that are derive from a set of long-term keys, yet discreet in nature
      * If one of the long term keys is compromised it doesn’t compromise the session key or the data it protects
    - Keys used to protect data aren’t used to derive additional key
      * Protects against multiple keys being decrypted
* Using appropriate Cryptographic Methods
  + WEP/WPA and WPA2
    - WEP can be cracked easily
      * RC4 stream cipher
    - WPA temporary replacement for WEP
      * RC4 with TKIP
    - WPA2 more secure
      * AES replaced RC4
      * CCMP replaced TKIP
    - WPA2 Enterprise
      * Includes RADIUS authentication
  + Hashing algorithm
    - MD5 = 128 bit
    - SHA 1 = 160 bit
    - SHA 256 = 256 bit
    - SHA 512 = 512 bit
    - HMAC
      * Hash-based message authentication code
      * Uses hashing function plus secret key
      * Hashing function that verifies integrity and authentication
  + Symmetric Key encryption
    - DES
      * Data Encryption Standard
      * 56-bit key
    - 3DES
      * Does 3 versions of DES implementation
    - AES
      * Advanced Encryption Standard
      * 128-bit fixed block size
      * Does 10 cycles of repetition for 128 bit keys
  + Asymmetric Key Encryption
    - RSA
      * Rivest, Shamir, Adleman
      * Digital Signatures
    - Diffie-Hellman
      * Keying material used to generate session keys
    - DHE
      * Ephemeral Diffie-Hellman
    - ECDHE
      * Elliptic-Curve Diffie-Hellman Ephemeral
  + One-time Pads
    - One-time pads are used for a single communication session and never reused again
    - Originated with sender and recipient having encryption key written on a pad of paper
    - Encryption key changed each time a communication was sent
  + NTLM/NTLMv2
    - NT LAN Manager
    - Used as authentication protocol in early Microsoft OS versions
    - NTML2 introduced with windows NT4
    - Kerberos replaced NTLM but NTM still used in certain situations
  + Blowfish
    - Symmetric key block cipher
    - Developed in 1993, still used today
    - 64 bit block size with variable key length from 32 bits to 448 bits
    - Originally designed as a fast, free replacement for DES, open source and patent/ license free
    - TwoFish and Three Fish are the recommended replacements for blowfish
  + PGP/GPG
    - “Pretty Good Privacy”
    - Developed in 1991, still in use
    - Concept of the Web of Trust
    - Don’t have to have a central ticket authority, can set up a web of people who trust each other
    - Combines several algorithms
      * Hashing
      * Data Compression
      * Symmetric key cryptography
      * Public – key cryptography
    - GPG (GNU Privacy Guard)
      * Open source and free
      * Implements the OpenPGP standard
      * Compatible with PGP
      * Supports RSA, DES, 3DES, etc.
      * Supports many graphical front ends
  + TwoFish
    - Successor to blowfish
    - Symmetric key block cipher
      * 128-bit block size and key sizes up to 256 bit
  + PAP and CHAP
    - Password Authentication Protocol should never be used, sends pw in clear text
    - Challenged handshake authentication protocol hashes PW’s
  + Strength and performance of algorithms
    - Symmetric
      * Faster than asymmetric
      * Same key for encryption and decryption
      * Bigger key sizes are more secure
      * Use more computational resources
      * Can be combined with asymmetric keys
    - Asymmetric
      * Public/private key
      * Bigger key sizes are more secure but use more resources
  + Transport Encryption
    - SSL
    - TLS
    - HTTPS, can be used in tandem with SSL/TLS
    - IPsec, used to secure communication over an insecure medium
    - SSH allows use to open a command prompt and act as if we were sitting locally
  + Cipher Suites
    - Strong vs. weak ciphers
    - Computational resources/capabilities continue to increase
    - Strong ciphers can become weak as computer power increases
    - Current strong cyphers:
      * AES
      * 3DES
      * TwoFish
    - Weak ciphers
      * WEP
  + Key Stretching- PKBDF2
    - Password based key derivation function 2
    - Part of RSA
    - Pseudorandom function applied to password or passphrase
    - Key stretching involves making passwords more secure by hashing, ciphers, or HMAC
    - Salt added as well for additional randomness
    - Process repeated many times
    - Eventually creates a derived key to be used in future communications
  + Key Stretching – Bcrypt
    - Based on Blowfish algorithm
    - Key derivation function used for passwords
    - Adds additional salt function to guard against rainbow table attacks
* PKI and Certificate Management
  + Certificate Authority
    - Has Public Key Infrastructure (PKI)
    - Secure Communication between sender/recipient
    - Communication over secure or insecure medium
    - Can be internal or external
    - Usually acts as a trusted third party between two actors
  + CRLs
    - Client Revocation List
    - Used to inform clients that certificates have been revoked/no longer valid
    - Can either hold (can be reinstated) or revoke a certificate
  + OCSP
    - Online Certificate Status Protocol
    - Used to obtain revocation status of x.509 digital certificates
    - Alternative to CRLs
  + CSR and PKCS Standards
    - Certificate Signing request
    - PKCS is most common
    - Public Key Cryptography Standards
    - Has basic information about entity requesting certificate
  + PKI
    - Public Key infrastructure
    - Components enable the usage of digital certificates and public key/private key encryption
    - Comprised of hardware, software, people, companies
    - Verisign and Thawte
  + Recovery Agent
    - Persona able to decrypt data encrypted by other users
    - Provides recovery capabilities if a user destroys credentials/keys, leaves the company
    - RA can recover any files/data encrypted while they are designated as the Recovery agent
  + Public Key
  + Private Key
    - If you encrypt with the public you will decrypt with the private, if you encrypt with the private you will decrypt with the public
    - Decrypting with the public ensures that the message came from the person you expected to send it
  + Registration
    - Verifies the identity of users requesting information from the certificate authority
  + Key Escrow
    - Trusted third party that holds the keys needed to decrypt data
    - Used in cases where keys are lost or some mandate requires the decryption of data
  + Trust Models
    - Hierarchical
      * Single root CA that digitally signs all certificates
      * Doesn’t scale well
    - Distributed Trust Model
      * Multiple CAs with one master root CA
      * Distributes load
      * Limits risk if one CA is compromised
    - Web of Trust
      * Used in smaller environments or end user communication with no centralized certificate authority
      * Commonly used with PGP encrypted communication where two parties with to communicate using self-generated keys