**Module 6 Cryptography & PKI**

**6.1 Crypto-Concepts**

**Encoding vs. Encrypting**

* Encrypting – plaintext/any data type concerted from readable form to encoded version that can only be decoded by another entity if they have access to decryption key
* Encoding – transforming data from 1 form to another using known algorithm so it can be reversed easily

1. No key required
2. Used to change human text into machine text (Eg. ASCII)

**Cryptography Definitions**

* Cryptography

1. Process of converting ordinary plain text into unintelligible text & vice-versa
2. Method of storing & transmitting data in particular form so only those whom its intended can read & process it
3. Confusion & Diffusion

* Algorithm – process/set of rules to be followed in calculations/other problem-solving operations
* Keys – secret value used within algorithm to encrypt & decrypt messages

**Symmetric Encryption**

* Same key for both encryption & decryption
* Secret/private key
* Advantages

1. Easier to implement
2. Faster

* Disadvantage – key distribution

**Symmetric Encryption Cipher**

* Block – chunks of data/fixed length group of bits

1. Requires padding if not enough data for block
2. Block size
3. More complex; not as fast
4. May require initialisation vector

* Stream – bits encrypted 1 at a time

1. Faster/higher performance
2. Susceptible to malicious insertions

**Key Strength**

* Length & complexity of key
* Longer = more secure
* Key entropy/randomness – generated through pseudo-random numbers
* Initialisation Vector (IV)

1. Fixed-size input of random/pseudo-random value
2. Ensures each message encrypts differently

* Nonce

1. Random/pseudo-random number used only once & associated with time stamp to increase key strength
2. Can be used as IV

**Key Exchange**

* Process & method for sharing encryption keys
* Especially when sender/receiver are distant
* In-Band – key shared in communications channel as message
* Out-of-Band – using another transmission media agreed upon in advance
* Forward Secrecy – if 1 key compromised, subsequent keys will not also be compromised (Perfect Forward Secrecy)

**Session & Ephemeral Keys**

* Session keys randomly generated to perform both encryption & decryption during communication of session between 2 parties

1. Valid only during that 1 communication session & is deleted

* Ephemeral keys

1. Also only used for 1 session
2. Common to ephemeral key agreement protocols

**Asymmetric Encryption**

* Uses 2 keys – 1 to encrypt, other to decrypt
* Keys mathematically related
* Public/private key encryption
* Only private key needs to be kept secret & only it can decrypt the message

**Digital Signatures/Nonrepudiation**

* Also uses public/private key pairs
* Message “signed” using sender’s private key
* Anyone can verify signature by using sender’s public key
* Used for repudiation (proof of origin)
* Used for message integrity (proof message hasn’t been altered)
* Doesn’t protect message confidentiality

**PKI (Public Key Infrastructure)**

* Set of roles, policies & procedures needed to manage public key (asymmetric) encryption
* Process of creating, managing, distributing, storing, using & revoke keys & digital certificates

**Hashing**

* “Digital Fingerprint”
* Work by taking string of any length & producing fixed-length string for output
* Hashing rules

1. Speed same no matter data size
2. Impossible to regenerate original message from its hash value
3. Avoid hash collisions – each message has unique hash
4. Changing original changes hash value

**Hashing Issues**

* Pre-computing hash values of common words (rainbow tables) – solved with a salt

1. Salting uses prefix consisting of random string of characters to passwords before they’re hashed

* Collision attacks tries to find 2 input strings of hash functions that have same output

**Elliptical Curve & Quantum Cryptography**

* Elliptical Curve Cryptography (ECC)

1. Asymmetric Public-Key cryptosystem based on complex mathematical structure
2. Uses smaller key sizes
3. Very fast

* Quantum Cryptography

1. Relies on physics rather than mathematics
2. Based on quantum state of photons
3. More secure

**Use of Proven Crypto Algorithms**

* National Institute of Standards & Technology (NIST) maintains publications & guidance for use of approved cryptographic & hashing algorithms
* Crypto best practices

1. Use well-known & approved cryptographic algorithms
2. Image adhere to required minimum key guidance for chosen algorithm
3. Image use approved cryptographic modes
4. Image use strong random number generators

**Obfuscation & Steganography**

* Obfuscation

1. Act of making something difficult to understand
2. Should rely on something not known/widely discovered
3. Does not provide strong security

* Steganography

1. Means “hidden writing”
2. Hiding messages, often in other media so unintended recipients not even aware of any message

**Crypto Use Cases**

* Confidentiality
* Integrity
* Availability
* Nonrepudiation
* State of data

1. Data at rest (stored)
2. Data in transit (across network)
3. Data in use (being processed)

**Common Crypto Use Cases**

* Low power devices
* Low latency
* High resiliency
* Supporting confidentiality
* Supporting integrity
* Supporting obfuscation
* Supporting authentication
* Supporting nonrepudiation
* Resource vs. security constraints