## Definitions

* **cryptosystem**: entire cryptographic operation. i.e. the key, algorithm, and key mgmt f’ns
* encryption and enciphering synonyms
* **key** or **cryptovariable** is the sequence that controls the operation of the cryptographic algorithm
* **work factor** represents the time and effort req’d to break a protective measure
* **initialization vector** nonsecret binary vector, used to introduce additional cryptographic variance and synchronize cryptographic equipment
* **transposition** or **permutation**: reorder plaintext
* **substitution**: exchange one letter for another
* **SP-network**: described by Claude Shannon, uses a series of S-boxes to handle the substitutions of the blocks of data. SP = “substitution and permutation”
* **confusion** provided by mixing the key values during repeated rounds
* **diffusion** provided by mixing up the location of the plaintext throughout the cipher text
* **avalanche effect** – a minor change in the key or plaintext will have significant effect on ciphertext
* transposition ciphers
* monoalphabetic and polyalphabetic ciphers
* modular mathematics and the running key cipher
* Vigenere cipher
* one-time pads
* steganography
* watermarking
* code words

## Symmetric Algorithms

* advantages: very fast, secure and cheap
* disadvantages: problems of key mgmt, does not provide many benefits beyond encryption

### DES – Data Encryption Standard, 1977

* key length is 64 bits, but effectively 56 bits.
* 2^56 relative strength

**Electronic Code Book (ECB)**

* each 64-bit block is encoded independently
* for 2 blocks the same, ciphertext would be the same
* allows random access files to be encrypted without processing in linear fashion
* used for very short messages (< 64-bits)

**Cipher Block Chaining Mode (CBC)**

* each input block will produce different output
* uses an IV and chaining XOR ciphertext block with next input block

**Cipher Feedback Mode (CFB)**

* input is broken to segments, IV loaded into shift register.
* encrypted, first 8 bits are XORed with first 8 bits of the plaintext.
* the resulting 8 bits are sent to receiver, then fed back into the shift register

**Output Feedback Mode (OFB)**

* like CFB, but sends first 8 bits of encrypted stream back into the shift register (instead of the XORed result)

**Counter Mode (CTR)**

* used in high speed applications, IPSec, ATM (Async Xfter Mode)
* a counter is a random 64-bit block, used as the IV
* next IV is ++counter, until entire message is encrypted

**Double DES**

* subject to meet-in-the-middle attacks
* known plaintext, known encrypted text. Brute force plain text with single DES and brute force ciphertext in the other direction until they match.

**3DES**

* relative strength of 2^112 for brute force
* C=E\_k1 ( E\_k2 ( E\_k1 (P))), called EEE2
* C=E\_k1 ( D\_k2 ( E\_k1(P))), called EDE2
* C=E\_k3 ( E\_k2 ( E\_k1 (P))), called EEE3
* C=E\_k3 ( D\_k2 ( E\_k1(P))), called EDE3

### AES – Advanced Encryption Standard, 1997

* be as strong as DES, larger block size, faster
* AES is Rijndael with 128-bit block

**Rijndael algorithm**

* varying block sizes: 128, 192, 256
* varying key length: 128, 192, 256
* variable number of rounds, depend on key length

**IDEA – International Data Encryption Standard, 1991**

* uses a 128-bit key, 64-bit blocks
* 8 rounds of substitution or permutation
* patents on IDEA will expire 2010-11

**Blowfish**

* developed by Bruce Schneier
* variable key sizes, from 32 up to 448 bits
* 64-bit input and output blocks

**RC5**

* Ron Rivest
* key varies from 0 to 2040 bits
* number of rounds is 0 to 255
* length is 16, 32, or 64 bit words (blocks)

**RC4**

* most widely used stream cipher
* used in WEP and SSL/TLS

## Asymmetric Algorithms

* uses a public and a private key
* slower than symmetric key algorithms
* **confidentiality**: message is encrypted with sent encrypted with the receiver’s public key. Only the receiver can decrypt it.
* **nonrepudiation**: *open message* – message is encrypted using the sender’s private key. It can be decrypted by anyone using the sender’s public key.
* sign and seal: provide confidential messages with proof of origin
  + sign message by encrypt with sender-private
  + seal message by encrypt with receiver-public

**RSA**

* based on difficulty of factoring product of two large primes
* C = P^e mod n
* p and q are chosen primes, p –ne q
* n = p\*q, choose e relatively prime to (p-1)(q-1)
* choose d < (p-1)(q-) such that ed = 1 mod (p-1)(q-1)
* public key {e, n} private key {d, n}

**Diffie Hellmann (key exchange) Algorithm**

* does not provide for message confidentiality
* based on discrete logarithms, must find the primitive root of a prime number

**El Gamal**

* based on work of Diffie Hellmann, but includes ability to do message confidentiality, and digital signatures (as well as key exchange)

**Elliptic Curve Cryptography (ECC)**

* speed and strength, highest strength per bit of key
* provide confidentiality, digital signatures, and message authentication

**Hybrid cryptography**: encrypt message with a symmetric key and send to receiver. Then encrypt the symmetric key with the receiver’s public key and send.

## Message Integrity Controls

**Checksums:**

* error detecting code, checksum or frame check
* used with symmetric key cryptography, the checksum is calculated and attached to the message. Both are then encrypted with a key

**Hash Function**

* accepts a message of any length and generates fixed length output, called a message digest
* must provide
  + assurance that the message cannot be changed without detection
  + impractical to find any two messages with the same has value
* Simple hash = block 1 XOR block 2 XOR …

**MD5, Ron Rivest 1992**

* most widely used hash algorithm
* 128 bit digest from message of any length
* used 512-bit blocks, four rounds of processing
* likelihood of finding any two messages with the same hash is one in 2^64
* a message for a given digest is 2^128

**MD4, 1990, 1992**

* 3 rounds of processing
* generates 128 bit output

**SHA Secure Hash Algorithm**

* based on MD4
* developed by NIST, 1993
* issued as FIPS (Federal Information Processing Standard) 180

**SHA-1**

* based on MD5
* uses 512-bit blocks, message length to 2^64
* output has is 160 bits
* four rounds of 20 steps

**FIPS 180-2 recognizes**

* SHA-256, SHA-384 and SHA-512

## Digital Signatures

## Encryption Management

## Public Key Infrastructure (PKI)

## Cryptanalysis and Attacks

(these sections are incomplete. Please add your own notes here!)

- signature contains message digest: to detect any alteration of the message

- effective key size of DES:

- Steganography can be defined as secret communication where the very existence of the message is hidden

- role of IKE within IPSEC protocol: Pear authentication and key exchange

- one way hash is the transformation of string Characters into a usually shorter fixed length.such transmission cannot be reversed

- Secure Electronic Transaction (SET): cryptographic protocol to send encrypted credit card numbers over the net.

- Directive of European Union on Electronic signatures deal with Non repudiation.

- Rijndal is encryption algorithm selected by NIST for the new Advanced Encryption standard.

- one-way hash provide Integrity

- Transposition and Substitution are 2 types of ciphers

- ISAKMP is the protocol to negotiate, establish, modify and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism

- WTLS offers security to wireless communications

- RC5 is a symmetric encryption alogorithm