

# Cryptography Terms

❖ *DigitalSherlock.com | SafeHack.com*

❖ *Date: 2005/05/27*

❖ *Document Name: cryptography\_terms.pdf*

❖ *GNU Free Documentation License*

❖ *Version 1.00, 2005-05-27*

❖ *Copyright © 2005 Adonis, MSc, Eng, CISSP, Security+, CEH, GSec, MCSE, etc.*

❖ *Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation.*

## ❖ A

### ➤ Avoidance controls

- **The separation of threats from assets and assets from threats.**

### ➤ Algorithm

- **The set of mathematical rules used in encryption and decryption**

## ❖ B

### ➤ Bitstream Authentication

- **Generate new MAC**
- **Compare with original**
- **Mac Algorithm qualities**
- **Sensitive to bit changes**
- **Creates MAC unable to be duplicated**

### ➤ Block Cipher

- **Breaks the plaintext into blocks and encrypts each with the same algorithm**
- **A block cipher is one that breaks a message up into chunks and combines a key with each chunk**
- **Apply an identical encryption algorithm and key to each block**
- **The properties of a cipher should contain confusion and diffusion**
- **Most modern ciphers are block ciphers**
- **Easy to implement in software (usually the width of data bus = 64 bits)**
- **Diffusion**
  - **Spread the plaintext character over many ciphertext characters. Done using permutations**
  - **Different unknown key values cause confusion**
  - **Putting the bits within the plaintext through many functions cause diffusion**
  - **N Accomplished through p-boxes**
  - **DES implements this product 16 times**
- **Confusion**
  - **Conceals statistical connection using substitution**
  - **N Accomplished through s-boxes**
  - **Block cipher use S-boxes**
  - **An S-box is non-linear because it generates a 4-bits output string from 6 bits input**

### ➤ Stream Cipher

- **Stream cipher treats the message as a stream of bits and performs mathematical functions on them individually**
- **Operate on small units of plaintext, bits**
- **Symmetric encryption**
- **Usually implemented in hardware**

- **Encrypts by operating on a continuous data stream**
- **A stream cipher is one that applies a key to each bit, one at a time**
- **Some stream cipher use stream generator**
- **Statistically unpredictable**
- **Much faster than any block cipher**
- **Effective Stream algorithm contains**
  - Long periods of no repeating patterns within keystream values
  - Statistically unpredictable
  - The keystream is not linearly related to the key

## ❖ C

### ➤ **Cipher**

- **A cryptographic transformation that operates on characters or bits**
- **Method of encrypting text (concealing its readability and meaning)**
- **Its origin is the Arabic sifr, meaning empty or zero**

### ➤ **Ciphertext**

- **An unintelligible message**
- **Ciphertext is encrypted text**
- **Data in encrypted or unreadable format**

### ➤ **Clustering**

- **A situation in which a plaintext message generates identical ciphertext messages by using the same transformation algorithm, but with different cryptovariables or keys.**
- **When two different keys generate the same ciphertext**
- **Plaintext message generates identical ciphertext using the same algorithm but different keys**

### ➤ **Code**

- **A cryptographic transformation that operates at the word or phrase level**

### ➤ **Cryptanalysis**

- **Practice of obtaining plaintext from ciphertext without a key or breaking the encryption**
- **Is the study of breaking cryptosystems**
- **The act of obtaining the plaintext or key from the ciphertext.**
- **Cryptanalysis refers to the study of ciphers, ciphertext, or cryptosystems to find bugs**
- **The Arabs invented cryptanalysis because of their expertise in mathematics.**

### ➤ **Cryptography**

- **Cryptography is the science of information security. The word is derived from the Greek kryptos, meaning hidden**
- **Science of secret writing that enables you to store and transmit data in a form that is available only to the intended individuals.**
- **Modern cryptography concerns**
  - Confidentiality
  - Integrity
  - Non-repudiation
  - Authentication
- **Applications of Cryptography**

### ➤ **Cryptology**

- **The study of both cryptography and cryptanalysis**

- **Cryptology is the mathematics, such as number theory, and the application of formulas and algorithms**
- **Cryptosystem**
  - **A set of transformations from a message space to ciphertext space**
  - **Hardware or software implementation of cryptography that transforms a message to ciphertext and back to plaintext**
  - **Example**
    - **M = plaintext**
    - **C = ciphertext**
    - **E = Encryption transformation**
    - **D = decryption transformation.**
    - **$E(M)=C$**
    - **$D[E(M)]=M$**
    - **$E(M,K) = C$**
    - **$D(C,K) = D[E(M,K),K] = M$**
- **Cryptovvariable or key**
  - **Information or a sequence that controls the enciphering and deciphering of messages**
- **Cryptographic algorithm**
  - **Are the mathematical rules that dictate the functions of enciphering and deciphering**
- **Clipper Chip**
  - **The Clipper chip contains the Skipjack encryption algorithm.**
  - **Each chip contains a unique 80-bit unit key U, which is escrowed in two parts at two escrow agencies**
  - **Was an encryption chip the US government wanted to implement into many American made devices so that they could listen to communication that contained suspected information**
  - **Clipper Chip - implemented in tamper proof hardware**
  - **Each clipper chip has a unique serial number and an 80 bit unique unit or secret key.**
  - **The Clipper Chip use The skipjack secret key algorithm which was developed by the NSA to enable the government to decrypt any traffic encrypted using the clipper chip**
  - **The chip is manufacture so that it cannot be reverse engineered**
  - **The problem with the clipper chip is that it has too weak a key at 80 bits and it has no public scrutiny.**
- **CAPSTONE chip**
  - **An integrated circuit with a Type II cryptographic processor that implements SKIPJACK, KEA, DSA, SHA,**
  - **Support asymmetric cryptography, and includes a key escrow feature.**
- **Certification Authority**
  - **Binds individuals to their public keys**
  - **Certificates are issued by certification authority**
  - **Certificates are digital documents attesting to the binding of a public key to an individual or other entity.**
  - **It contains the digital signature of the certificate issuer**
- **Cryptographic Module Configurations There is four type of modules**
  - **Inline**
    - **Front end configuration**
    - **Module capable of accepting plaintext from source**

- Performing crypto processing
- Passing processed data directly to communications equipment
- Without passing back to source
- May also decrypt reverse process
- Data cannot leave host without passing through module
- Comm equip in module or external to host
- **Offline**
  - Back end configuration
  - Module capable of accepting data from source
  - Performing crypto processing
  - Passing processed data back to source
  - Source responsible for storage and further transmission
  - Maintaining separation between protected and unprotected data
  - Ideal for local file encryption
  - Comm boards may be internal to host
- **Embedded**
  - Module physically enclosed within and interfaces with computer
  - Either inline or offline
  - Less expensive
  - Physical security (temper protection and detection) questionable
- **Standalone**
  - Module contained in own physical enclosure
  - Outside host computer
  - Either inline or offline
- **Commercial COMSEC Endorsement Program (CCEP)**
  - Introduced by NSA in the mid-80's
  - Combine government crypto knowledge with industry product-development expertise
- **Collision**
  - In one-way hash (MD5), finding two messages that hash to the same value is known as a collision
  - Can be exploited using
    - Brute force Attack
    - Birthday attack

## ❖ D

- **Decipher**
  - The process of decryption transforms ciphertext back into the original plaintext
  - To undo the encipherment process and make the message readable
  - Act of transforming data into a readable format
  - All three terms - decipher, decrypt, and decode - mean to convert ciphertext into the original,
- **DNSSEC**
  - Is Domain Name Server Security and was designed to secure distributed name services.
- **Digital envelope**
  - A digital envelope for a recipient is a combination of encrypted content data (of any kind) and the content encryption key in an encrypted form that has been prepared for the use of the recipient

- **Digital certificate**
  - A certificate document in the form of a digital data object (a data object used by a computer) to which is appended a computed digital signature
- **Digital signature**
  - A method for verifying that a message originated from a principal and that it has not changed en route.
  - Encrypting a digest of the message with the private key of the signing party typically performs digital signatures.
  - A non-forgeable transformation of data that allows the proof of the source (with non-repudiation) and the verification of the integrity of that data.
- **Digital signature algorithm (DSA)**
  - Is an asymmetric cryptographic algorithm that produces a digital signature in the form of a pair of large numbers.
  - This algorithm uses a private key to sign a message and a public key to verify the signature.
  - It is a standard proposed by the U.S. Government.
  - DSA is used to Digitally sign the message
- **Digital System Encryption**
  - The key and message both streams of bits
  - Each text character = 8 bits
  - Each key bit XORed (exclusived-or'ed) with corresponding message bit
  - XOR operation yields 0 if both bits the same and 1 is different
  - Example:
    - MESSAGE STREAM 01001000
    - KEY STREAM 11010001
    - CIPHERTEXT STREAM 10011001

## ❖ E

- **Export Issues regarding Encryption**
  - Cryptography is just one of many technologies which is covered by the ITAR (International Traffic in Arms Regulations)
  - U.S allow 56-bit block ciphers to be exported
- **Encipher**
  - To make the message unintelligible to all but the intended recipients
  - Its purpose is to ensure privacy by keeping information hidden
  - The process of Encryption turns plaintext into ciphertext
  - Act of transforming data into an unreadable format
- **End-to-end encryption**
  - Encrypted information that is sent from the point of origin to the final destination
- **Electronic Document Authorization (EDA)**
  - Authorizes certificates
  - Specifies public key holder authority/power
  - Spend, authorize payments, perform business functions
  - Specifies limits to prevent abuse

## ❖ F

- **Fair Cryptosystems**

- Separate the necessary key required for decryption this method take place in the software encryption processes using public key cryptography

## ❖ G

## ❖ H

## ❖ I

## ❖ J

## ❖ K

### ➤ Keyspace

- The range of possible keys is referred to as the keyspace
- Possible values used to construct keys
- A larger keyspace and the full use of the keyspace allows more random keys to be created

### ➤ Key Escrow

- The unit keys are split into two sections and are given to two different escrow agencies to maintain
- Different agencies or entities, hold onto the different pieces and come together when decryption is necessary
- Key escrow is a practice that splits up the necessary key required to decrypt information
- Allowing law enforcement to obtain the keys to view peoples encrypted data
- Court order to get both pieces
- The escrowed encryption standard is embodied in the US governments Clipper Chip,
- The 80 bit key of the clipper chip is weak.
- Key escrow is mainly used when hardware encryption chips
- Key escrow approach is fair cryptosystems.
- Used when hardware encryption chips are used

### ➤ Key

- A key is a random string of bits that is inserted into an encryption algorithm
- Secret sequence of bits and instructions that governs the act of encryption and decryption
- The results determines what encryption functions will be carried out on a message and in what order
- In symmetric key algorithms the sender and receiver use the same key for encryption and decryption
- In asymmetric key algorithms the sender and receiver use different keys for encryption and decryption
- If a message is encrypted with public key, it is decrypted with a private key and vice versa

### ➤ Key clustering

- Instance when two different keys generate the same ciphertext from the same plaintext

## ❖ L

### ➤ Logical Operation

- AND

- The output is "true" when both inputs are "true." Otherwise, the output is "false."
- **OR**
  - The output is "true" if either or both of the inputs are "true." If both inputs are "false," then the output is "false."
- **XOR**
  - The output is "true" if either, but not both, of the inputs are "true." The output is "false" if both inputs are "false" or if both inputs are "true."
  - $0+0=0$ ,  $0+1=1$ ,  $1+1=0$ ,  $1+1=0$
  - Boolean Operation
  - Indicated by XOR
  - Indicated by symbol circle +
  - Easily implemented in hardware
- **NOT**
  - It reverses the logic state
- **NAND**
  - The output is "false" if both inputs are "true." Otherwise, the output is "true."
  - The NAND gate operates as an AND gate followed by a NOT gate
- **NOR**
  - The NOR gate is a combination OR gate followed by an inverter
  - Its output is "true" if both inputs are "false." Otherwise, the output is "false."
- **XNOR**
  - Its output is "true" if the inputs are the same, and "false" if the inputs are different.
  - The XNOR (exclusive-NOR) gate is a combination XOR gate followed by an inverter

### ➤ **Link Encryption**

- **Each entity has keys in common with its two neighboring nodes in the transmission chain**
- **N Node 1 -Encrypts with key A**
- **N Node 2 - Decrypts with key A and encrypts with key B**
- **N Node 3 - Decrypts with Key B and encrypts with Key C**

## ❖ **M**

### ➤ **Message authentication code VS. Code Generation**

- **Message Authentication**
- **MAC Generation**

### ➤ **MAC**

- **A message authentication code (MAC)**
- **It is an authentication tag**
- **MACs are computed and verified with the same key**
- **Hash function-based MACs (often called HMACs)**
- **There are four types of MACs**
  - Unconditionally secure
  - Hash function-based
  - Stream cipher-based
  - Block cipher-based

## ❖ **N**

### ➤ **NonRepudiation**

- **Ensures sender can't deny sending**

- Recipient can't deny claim that they received something else

## ❖ O

## ❖ P

### ➤ Plaintext

- Is ordinary readable text before being encrypted into ciphertext
- Data in readable format, also referred to as cleartext

### ➤ Prime numbers

- A prime number has no whole-number factors other than 1 and itself.
- The first ten prime numbers are: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29.
- No one has yet found a pattern or formula for counting indefinitely by primes.

### ➤ Polyalphabetic

- Polyalphabetic cipher use more than one alphabet to defeat frequency analysis

## ❖ Q

## ❖ R

## ❖ S

### ➤ Substitution

- Change a character (or bit) out for another

### ➤ Split knowledge procedures

- Similar to separation of duties, as one person alone does not have all the knowledge or access to the keys to cause damage.
- The knowledge and access is distributed.

## ❖ T

### ➤ Transposition

- Scramble the characters (or bits)

## ❖ U

## ❖ V

## ❖ W

### ➤ Work Function (Factor)

- Estimated time, effort, and resources necessary to break a cryptosystem
- Difficulty in recovering plain text from ciphertext as a factor of time and cost
- Systems security is directly proportional to the work function
- Work function should be commensurate with the value of the data

## ❖ X

## ❖ Y

## ❖ Z

### ➤ Zeroization

- A method of erasing electronic data by altering the contents so that recovering the data is not possible.

### ➤ Zero Knowledge proof

- This is when one party can reveal something to a second party without revealing any

additional information.

➤ **Zero knowledge protocol**

- The following are all primary features of a zero knowledge protocol
- A.) The verifier can not learn anything from the protocol
- B.) The prover can not cheat the verifier
- C.) The verifier can't cheat the prover
- Zero-knowledge protocols allow identification, key exchange and other basic cryptographic operations to be implemented without leaking any secret information during the conversation