Network Defence (BUW 3333)

Tutorial 4

1. Define the following terms in the context of cryptography:
2. Plaintext

Plaintext is a term used in cryptography that refers to a message before encryption or after decryption.

1. Ciphertext

Ciphertext is the unreadable output of an encryption algorithm which uses cipher as an algorithm to get ciphertext.

1. Key

Key, which is also known as cryptographic key is a string of bits used by a cryptographic algorithm to transform plain text to cipher text or vice versa. This key remains private and ensures secure communication.

1. Encipher (encrypt)

It is a method that converts information into secret code that hides the information’s true meaning. It converts plaintext to ciphertext.

1. Decipher (decrypt)

It is a method that recovers plaintext from ciphertext.

1. Cryptanalysis

It is also known as code breaking. It is a study of principles/methods of deciphering ciphertext without knowing key.

1. Cryptology

Cryptology is a field of both cryptography and cryptanalysis.

1. What is the difference between symmetric and asymmetric cipher?

Symmetric cipher is a single-key, secret-key or conventional encryption which are used by both sender and receiver. They both use the same key.

Asymmetric cipher is a two-key or public-key encryption if the sender and receiver each use the different key.

1. What are the two requirements for secure use of symmetric encryption?

The two requirements are a strong encryption algorithm as well as sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.

1. How many keys are required for two people to communicate via a symmetric cipher?

Only 1 key is required as both sender and receiver use the same key.

1. What is the difference between a block cipher and a stream cipher?

Block cipher processes the input one block of elements at a time and produces an output block for each input block.

Stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

1. List and briefly describe the Feistel cipher design elements?

|  |  |
| --- | --- |
| Elements | Description |
| Block size | Larger block sizes mean greater security but reduced encryption / decryption speed |
| Round function | Greater complexity generally means greater resistance to cryptanalysis. |
| Key size | Larger key size means greater security but may decrease encryption/decryption speed |
| Fast software encryption/decryption | In many cases, encryption is embedded in applications or utility functions in such a way as to preclude a hardware implementation; accordingly, the seed of execution of the algorithm becomes a concern. |
| Number of rounds | The essence of a symmetric block cipher is that a single round offers inadequate security but that multiple rounds offer increasing security. |
| Subkey generation algorithm | Greater complexity in this algorithm should lead to greater difficulty of cryptanalysis. |
| Ease of analysis | If the algorithm can be concisely and clearly explained, it is easier to analyze that algorithm for cryptanalytic vulnerabilities and therefore develop a higher level of assurance as to its strength. |

1. What are the three most commonly used symmetric block ciphers?

Data Encryption Standart (DES), Advanced Encryption Standard (AES) and Triple DES (3DES).

1. Briefly describe what Message Authentication is.

Message Authentication is an encryption protects against passive attack (eavesdropping) to protect against active attack which are falsification of data and transactions. It is a procedure that allows communicating parties to verify that received messages are authentic.

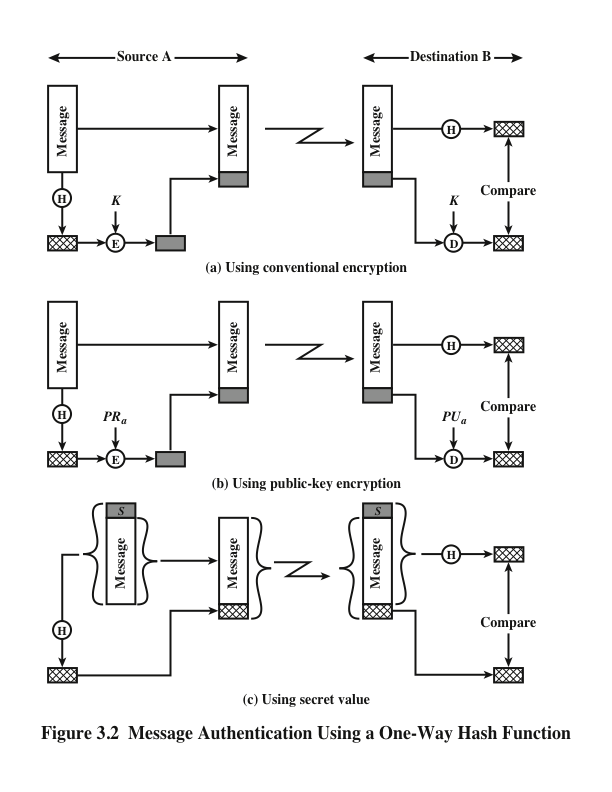
1. What are the main/important aspects of message authentication?

One of the aspects is to verify that the contents of the message have not been altered. Besides that, the source is authentic. It also verifies a message’s timeliness (it has not been artificially delayed and replayed) and sequence relative to other messages flowing between two parties.

1. Draw the diagram and explain step-by-step the process of message authentication using a Message Authentication Code (MAC).



1. Sends original message and MAC (H1).
2. At receiver end, it receives the original message and MAC.
3. The receiver calculates MAC (H2) using key and original message.
4. Compare H1 and H2.
5. If H1 != H2, then message altered.
6. If H1 == H2, then message not changed.
7. Draw the diagram and explain step-by-step the process of message authentication using a One-Way Hash Function.



1. The sender writes hash function into the authentication tag.
2. The receiver runs the same computation and checks the result against the tag.
3. If the two do not match, the message authentication is said to fail and the packet is discarded.
4. Identify the three main techniques in which hash functions are used for message authentication.

Using conventional encryption, public-key encryption and secret value.

1. State the main difference between MAC algorithms and one-way hash functions.

The main difference between MAC algorithms and one-way hash functions is that the MAC algorithms are used to guarantee integrity and authentication whereas hash guarantees the integrity of data. Hashcode is blindly generated from the message without any kind of external input. A MAC instead uses a private key as the seed to the hash function it uses when generating the code.

1. What are the roles of the public and private key?

Two keys are used in public key, one key is for encryption whereas another key is for decryption. Whereas the same key in private key is used for both encryption and decryption.

1. Briefly describe the two most common misconceptions about public-key encryption.

One of the misconceptions is public-key encryption is more secure from cryptanalysis than conventional encryption. Another misconception is the public-key encryption is a general-purpose technique that has made conventional encryption obsolete.

1. What are three broad categories of applications of public-key cryptosystems?

The three broad categories of applications of public-key cryptosystems are encryption/decryption, digital signature and key exchange.