Hi, I'm Mike Chapple and this is the audio review of the study essentials for chapter 6 of the official CISSP study guide. Here are the top things you need to know from this chapter on cryptography and symmetric key algorithms.

Understand the role that confidentiality, integrity and non-repudiation play in cryptosystems. Confidentiality is one of the major goals of cryptography. It protects the secrecy of data, while it is both at rest and in transit. Integrity provides the recipient of a message with the assurance that data was not altered intentionally or unintentionally between the time it was created and the time it was accessed. Non-repudiation provides undeniable proof that the sender of a message actually authored it. It prevents the sender from subsequently denying that they sent the original message. Know how cryptosystems can be used to achieve authentication goals. Authentication provides assurances as to the identity of a user. One possible scheme that uses authentication as the challenge response protocol in which the remote user is asked to encrypt a message using a key known only to the communicating parties. Authentication can be achieved with both symmetric and asymmetric cryptosystems.

Be familiar with the basic terminology of cryptography. When a sender wants to transmit a private message to a recipient, the sender takes a plain text unencrypted message and encrypts it using an algorithm and a key. This produces a ciphertext message that is transmitted to the recipient. The recipient then uses a similar algorithm and key to decrypt the ciphertext and recreate the original plain text message for viewing.

Understand the difference between a code and a cipher and explain the basic types of ciphers. Codes are cryptographic systems of symbols that operate on words or phrases and are sometimes secret, but don't always provide confidentiality. Ciphers, however, are always meant to hide the true meaning of a message. Know how the following types of ciphers work. Transposition ciphers, substitution ciphers, including one-time pads, stream ciphers and block ciphers. Know the requirements for successful use of a one-time pad. For a one-time pad to be successful, the key must be generated randomly without any known pattern. The key must be at least as long as the message to be encrypted, the pads must be protected against physical disclosure and each pad must be used only one time and then discarded.

Understand split knowledge. Split knowledge means that the information or privilege required to perform an operation is divided among multiple users. This ensures that no single person has sufficient privileges to compromise the security of the environment. M of N control is an example of split knowledge used in key recovery and other sensitive tasks.

Understand work function or work factor. Work function or work factor is a way to measure the strength of a cryptographic system by measuring the effort in terms of cost and or time to decrypt messages. Usually, the time and effort required to perform a complete root force attack against an encryption system is what a work function rating represents. The security and protection offered by a cryptosystem is directly proportional to the value of it's work function or work factor.

Understand the importance of key security. Cryptographic keys provide the necessary element of secrecy to a cryptosystem. Modern cryptosystems utilize keys that are at least 128 bits long to provide adequate security. Know the differences between symmetric and asymmetric cryptosystems. Symmetric key cryptosystems or secret key cryptosystems rely on the use of a shared secret key. They are much faster than asymmetric algorithms, but they lack support for scalability, easy key distribution and non-repudiation.

Asymmetric cryptosystems use public private key pairs for communication between parties, but

operate much more slowly than symmetric algorithms. Be able to explain the basic operational modes of symmetric cryptosystems. Symmetric cryptosystems operate in several discrete modes, including electronic code book mode, cipher block chaining mode, cipher feedback mode, output feedback mode, counter mode, Galois counter mode and counter with cipher block chaining message authentication code mode.

Electronic code book mode is considered the least secure and is used only for short messages. Triple DES uses three iterations of DES with two or three different keys to increase the effective key strength to 112 or 168 bits. Know the advanced encryption standard, AES. AES uses the Rijndael algorithm and is the US government standard for the secure exchange of sensitive but unclassified data. AES uses key links of 128, 192 and 256 bits and a fixed block size of 128 bits to achieve a much higher level of security than that provided by the older DES algorithm. Those are the study essentials that you'll need to know for chapter 6, cryptography and symmetric key algorithms.

From:
https://trident365.com/ - **三叉戟**

Permanent link:
https://trident365.com/doku.php?id=projects:cissp:chapter6

Last update: **2025/05/18 17:15**