9.5.2 Symmetric Encryption Facts

Symmetric key encryption, also known as secret key encryption, pre-shared key, or private key encryption, uses only one key to encrypt and decrypt data.

- Symmetric-key encryption is a form of cryptography that provides confidentiality with a weak form of authentication or integrity.
- Symmetric encryption is well-suited for bulk encryption of less sensitive data because it is less CPU-intensive than other encryption methods.
- Before communications begin, both parties must exchange the shared secret key using a secure channel. Symmetric-key encryption uses the following key distribution methods:
  - Out-of-band distribution involves manually distributing the key, such as copying the key to a USB drive and sending it to the other party.
  - In-band distribution uses mechanisms such as the following to distribute the key:
    - Using a key distribution algorithm such as Diffie-Hellman
    - Using asymmetric technology to encrypt the key for distribution
- Each pair of communicating entities requires a unique shared key. This means that the number of keys required grows exponentially as the number of communication partners grows. For example, 1,000 users in a system would require the generation of almost 500,000 different keys.
- The key space is typically short, ranging from 56 bits to a maximum of 512 bits. (As the number of bits in the key increases, so does the strength of the encryption; however, this increase also requires more CPU resources to perform the encryption.)
- Having two copies of each key makes it harder to secure the keys.

Symmetric encryption uses two algorithm types:

Type	Description
Block	Block ciphers encrypt by transposing plaintext to ciphertext in chunks (block by block). Block ciphers: ▪ Are fast. ▪ Can process large amounts of data. They do not process small amounts of data well. ▪ Are typically implemented in software. ▪ Use a substitution and transposition function. ▪ Apply several alternating rounds of substitution and transposition. A round refers to data going through one substitution and transposition process. ▪ May begin to show patterns in the cipher when processing large amounts of data. ▪ Can be strengthened by implementing an Initialization Vector (IV) at the start of the encryption process.
Stream	Stream ciphers use a sequence of bits known as a keystream, which is the key used for encryption. The encryption is performed on each bit within the stream in real time. Common uses for symmetric-key stream ciphers include ATM card PINs and smart cards. Stream ciphers: ▪ Are best used for small amounts of data, usually less than 64 bits ▪ Are slower than symmetric key block ciphers ▪ Are best implemented in hardware because the data size makes it infeasible to have enough RAM or CPU cycles to process the data ▪ Use bitwise functions in which the cipher is calculated on the individual bits in the datastream ▪ Use a keystream generator to produce long streams of bits with no patterns ▪ Are capable of block cipher emulation and can be used with block ciphers The most frequently used implementation of symmetric key stream ciphers is Ron's Code (or Ron's Cipher) v4, known as RC4. RC4: ▪ Uses a variable key up to 256 bits ▪ Is commonly used with WEP and SSL ▪ Uses the Key Scheduling Algorithm (KSA) and the Pseudo-Random Generation Algorithm (PRGA) Basic Encoding Rules (BER) are the original rules for encoding abstract information into a concrete data stream. BER specifies a set of self-identifying and self-delimiting schemes that allow each data value to be identified, extracted, and decoded individually.

Common symmetric cryptography methods include:

Method	Characteristics
Ron's Cipher v2 or Ron's Code v2 (RC2)	RC2 is a variable-key-sized block cipher that was designed to replace DES. RC2 was produced by RSA Security, Inc. RC2: ▪ Uses 64-bit blocks. ▪ Uses 8 to 128-bit keys in 8-bit increments. ▪ Uses salt, which is used to modify a password hash by using a random string of data to prohibit password hash matching types of attacks.
Ron's Cipher v5 or Ron's Code v5 (RC5)	RC5 is a symmetric-key block cipher cryptographic algorithm produced by RSA Security, Inc. RC5: ▪ Supports 32-, 64-, or 128-bit blocks

	▪ Supports key sizes 0–2K ▪ Can implement up to 255 rounds of substitution and transposition ▪ Supports variable bit length keys and variable bit block sizes The parameters of RC5 increase its variability, making it more difficult to crack.
International Data Encryption Algorithm (IDEA)	International Data Encryption Algorithm, originally called Improved PES, is a minor revision of an earlier PES (Proposed Encryption Standard). IDEA: ▪ Uses 64-bit blocks with 128-bit keys ▪ Is used by Pretty Good Privacy (PGP) email encryption ▪ Is an optional algorithm in OpenPGP ▪ Does not support variable block size
Data Encryption Standard (DES)	Data Encryption Standard is a very popular encryption standard created by the NSA. DES: ▪ Was one of the first symmetric encryption methods and is now obsolete (known weaknesses can be used to break the encryption) ▪ Was adopted by the government for sensitive but unclassified encryption ▪ Uses data encryption algorithm with a 56-bit key and 8-bit parity ▪ Implements a 64-bit block size with 16 rounds of substitution and transposition ▪ Is used in IPsec as its weakest and fastest encipherment ▪ Can be easily broken DES has four primary modes: ▪ The Electronic Code Book (ECB) is a mode in which each block of text is run through the DES encryption and cipher text is created. This mode is the weakest because it is subject to patterns. It is best used on small amounts of data or on data that is not highly sensitive. ▪ The Cipher Block Chaining (CBC) mode increases randomness. ▪ The Output Feedback (OFB) mode adds stream emulation and works with block ciphers such as DES. ▪ The Cipher Feedback (CFB) mode strengthens OFB by increasing the randomness and variability of the cipher text.
Triple DES (3DES)	Triple DES is an enhanced version of DES. Triple DES: ▪ Applies DES three times ▪ Uses a 168-bit key ▪ Is used in IPsec as its strongest and slowest encipherment Encrypting large amounts of data tends to create patterns in the ciphe text. There are two implementations of 3DES used to create strong ciphertext by using multiple keys: ▪ EDE2 encrypts with key1, then decrypts with key2, and finally encrypts again with key1. ▪ EEE3 encrypts with key1, then encrypts with key2, and finally encrypts with key3.
Advanced Encryption Standard (AES)	Advanced Encryption Standard is an iterative symmetric-key block cipher that was developed as a replacement to DES in 2001. AES: ▪ Uses the Rijndael Block Cipher, which is resistant to all known attacks ▪ Uses a variable-length block and key length (128-, 192-, or 256-bit keys) ▪ Is stronger and faster than 3DES when implemented with a large key size (256-bits) ▪ Was selected as the method to replace DES
Blowfish	Blowfish is a keyed symmetric block cipher that was intended to be free of the problems associated with other algorithms and replace DES. Blowfish: ▪ Uses 64-bit blocks and key lengths anywhere from 32 to 448 bits ▪ Has no effective known cryptanalysis currently
Twofish	The Twofish symmetric block cipher permits a wide variety of tradeoffs between speed, software size, key setup time, and memory. Twofish: ▪ Uses 128-bit blocks and variable key lengths (128-, 192-, or 256-bits) ▪ Uses up to 16 rounds of substitution and transposition ▪ Was the runner up to Rijndael in the selection of the algorithm of AES
SkipJack	SkipJack was created by the National Security Agency (NSA). SkipJack: ▪ Encrypts 64-bit blocks of data with an 80-bit key ▪ Uses the Clipper chip (Very Large Scale Integration) device with an Advanced RISC Machine (ARM)

	▪ Became unpopular when a backdoor was discovered that allowed the NSA to decrypt all messages produced by the Clipper chip

Using longer keys reduces the possibility of successful attacks by dramatically increasing the number of possible unique key combinations. Increasing the size of a symmetric key by just one bit doubles the amount of effort that is required to conduct an exhaustive key search attack. Doubling the size of the key actually squares the amount of effort required to discover the key. Consider the following examples:

- Using a 40-bit key allows a total of 2^{40} possible unique key combinations. If an attacker uses a computer that can generate one million keys every second to discover the correct key, it will take approximately two weeks to generate all possible keys.
- Using a 128-bit key allows a total of 2^{128} possible unique key combinations. If an attacker uses a computer that can generate one million keys every second to discover the correct key, it would take billions of years to generate all possible keys.

Key stretching strengthens weak encryption keys against exhaustive key search attacks. In many encryption implementations, such as Wi-Fi Protected Access (WPA2), the shared secret is a password or pass phrase that was created by a human, which can frequently be short and predictable enough to be cracked. Key stretching addresses this issue by making keys more complex, causing exhaustive key search attacks to be much more difficult.

Using key stretching, the initial key is fed into an algorithm that enhances it to create a stronger key. The enhanced key is usually at least 128 bits long, making it almost impossible to crack. Several commonly used key stretching algorithms include the following:

- PBKDF2
- bcrypt
- scrypt

Keyed-hash Message Authentication Code (HMAC) embeds a symmetric key into a message before the message is hashed. When the message is received, the recipient's symmetric key is added back into the message before hashing the message. If the hash values match, message integrity is proven. HMAC:

- Can use any hashing function, although more secure hashing functions are preferable, including SHA-1, MD5, and RIPEMD.
- Is suitable anytime senders and receivers wish to guarantee integrity between sender and receiver.
- May not be used for non-repudiation; both sender and receiver can correctly generate an HMAC output.
