7.1.5 Symmetric and Asymmetric Encryption Facts

Encryption is the process of encoding data into something that is unreadable called ciphertext. All encryption processes rely on using a unique key. The encryption key is basically a password that is combined with the cipher to encrypt the data.

This lesson covers the following topics:

- Symmetric encryption
- Asymmetric encryption
- Hybrid cryptosystems
- Ephemeral keys

Symmetric Encryption

Symmetric encryption uses the same key to encrypt and decrypt data. This is the simplest and oldest form of encryption.
One of the main drawbacks of symmetric encryption is that the key must be shared before a user can decrypt a message.
If the key needs to be shared with multiple people, the integrity of the key is compromised as it becomes easier for a hacker to steal the key.

Symmetric encryption is extremely secure when the key is kept safe. This form of encryption is useful when a large amount of data needs to be encrypted as the encryption process requires less CPU power than other encryption methods.

The table below shows some of the more common symmetric key algorithms in use.

Symmetric Algorithm	Description
Data Encryption Standard (DES)	The DES family of ciphers was first developed in the early 1970s by IBM. ▪ DES was heavily used through the 1990s until hackers figured out how to brute-force the keys. ▪ Triple-DES (3DES) was introduced in 1998. This version combined 3 different keys, giving it a key length of 168 bits. ▪ 3DES is extremely CPU heavy and is not used much today.
Rivest's Cipher (RC)	The RC family of algorithms were developed by Ron Rivest in 1987. ▪ RC4 was once the most used cipher. However, many vulnerabilities have since been found and it is no longer supported. ▪ RC6 is the latest version and is a 128-bit cipher.
Advanced Encryption Standard (AES)	AES, also known as the Rijndael cipher, was developed by Jaon Daemen and Vincent Rijmen in 2001 as part of a NIST competition held to find a replacement for DES. ▪ AES has essentially replaced all other types of symmetric encryption. ▪ AES offers three different key lengths of 128, 192, and 256 bits. ▪ AES is used in many different applications including 802.11 communications,

	Bitlocker, and even game engines.
International Data Encryption Algorithm (IDEA)	IDEA was first developed in 1991 by James Massey and Xuejia Lai. ▪ IDEA was used in Pretty Good Privacy (PGP) 2.0 and is an optional algorithm in the OpenPGP standard. ▪ IDEA uses a 128-bit key.
Blowfish	Blowfish was developed in 1993 by Bruce Schneier. It was meant to be a replacement for DES. ▪ Blowfish is unpatented so that it can be used freely by anyone. ▪ Blowfish uses a 128-bit key. ▪ Vulnerabilities have been discovered in the Blowfish cipher and it is recommended to use its successor, Twofish, instead.
Twofish	Twofish was one of the five finalists for the AES contest but ultimately was not chosen. ▪ Twofish uses keys up to 256 bits in size. ▪ Twofish is slower than AES.
CAST	CAST is a family of ciphers that now consists of CAST-128 (CAST5) and CAST-256 (CAST6). ▪ CAST5 is the most widely used CAST cipher. It replaced IDEA in PGP 3.0 and is also an option in all versions of Open PGP. ▪ CAST6 was entered in the AES competition but was not a finalist.

Asymmetric Encryption

Asymmetric encryption uses two keys instead of one. A user's public key is used to encrypt the data. That user then uses their private key to decrypt the data. The private key only decrypts data that was encrypted using its matching public key.

Asymmetric encryption is used in most communication over the internet. The following is an example of how asymmetric encryption is used:

1. When a user wants to log into a website, the browser sends a request to the web server for the public key.
2. The user's login information is encrypted using the public key and sent to the server.
3. The server uses its private key to decrypt the user's login information.

Asymmetric encryption is also used to create digital signatures.

- By using a private key along with a hash of the data being sent, a digital signature is created.
- The recipient can verify the digital signature to ensure the message is legitimate and actually comes from the sender.
- Digital signatures are not meant to encrypt or secure data. Their main function is to provide non-repudiation, which means the sender cannot deny having sent the message. Digital signatures are also used to verify that the data transmitted was not changed or corrupted.

The following table shows the four main asymmetric encryption algorithms:

Asymmetric Algorithm	Description
Diffie-Hellman	Released in 1976 by Whitfield Diffie and Martin Hellman. Its purpose was to allow two users who have never met to safely create a shared key over a public channel such as the internet. ▪ Diffie-Hellman is used as follows: 1. The two users agree on two numbers, a prime number (P) and a generator (g). These numbers can be shared publicly. 2. Each user then randomly generates a private number, or key, unique to themselves. 3. Using the prime number, generator, and private key, each user generates a public key using the following formula: ▪ (G^ private number) MOD P 4. The users exchange their public keys which are then used to create a shared secret key using the following formula: ▪ (Shared Public Key^ private number) MOD P 5. Because each public key was generated using the same prime number and generator, each user will come up with the same number for the shared secret key. 6. If a hacker intercepted any of the exchanges, they wouldn't be able to reverse the process without knowing each user's secret number. ▪ Diffie-Hellman is frequently implemented in security protocols such as TLS, IPSec, SSH, and others.
Rivest-Shamir-Adleman (RSA)	RSA was developed by Ron Rivest, Adi Shamir, and Leonard Adleman. RSA was released shortly after Diffie-Hellman in 1977. ▪ RSA is still one of the most commonly used algorithms and helped defined the process of using a public key to encrypt data and a private key to decrypt the data. ▪ RSA is used extensively for creating digital signatures.
Digital Signature Algorithm (DSA)	DSA was proposed in 1991 by NIST and became the government standard in 1993 ▪ DSA is only used for creating digital signatures. ▪ It uses a different algorithm than RSA but provides the same level of security.
Elliptic Curve Cryptography (ECC)	Elliptic Curve Cryptology is one of the newer methods being implemented. It was originally introduced in 1985. It did not enter wide usage until 2004. ▪ ECC is able to generate smaller keys that are more secure than most other methods. ▪ Many websites today use ECC to secure connections and data transmissions.

Hybrid Cryptosystems

Hybrid cryptosystems combine the efficiency of symmetric encryption with the convenience of asymmetric encryption. A hybrid cryptosystem is used as follows:

1. User1 uses their symmetric private key to encrypt some data.

2. User1 then encrypts that symmetric private key using the recipient's public key and sends both to the recipient.
3. User2, the recipient, uses their private key to decrypt User 1's private key which is then used to decrypt the message.
4. As long as User2's private key is kept secret, the data remains secure.

Hybrid cryptosystems are used with many secure communication methods today such as TLS.

Ephemeral Keys

In traditional encrypted communications, static keys are used. This means that the same key is used throughout an entire session. The problem with this is that the longer the keys are used, the more susceptible they become to an attack. Ephemeral keys can be used to resolve this issue.

Ephemeral keys are keys that are generated for each new session or message sent. For example, perfect forward secrecy (PFC) uses ephemeral keys.

Some popular instant messaging apps make use of ephemeral keys to encrypt messages. Each message sent uses a unique key to encrypt it. If a hacker intercepts one key, the rest of the messages are still safe.