9.2.2 Advanced Cryptography Facts

Advanced cryptography includes the following:

Concepts	Definition
Encrypting	The purpose of encryption is obfuscation, making a message obscure so it is difficult to read. ▪ Cryptographic service providers (CSPs) are software libraries that can be used to enhance encryption. Applications can use these libraries to help secure email and provide strong user authentication.
Key Exchange	The sender of an encrypted message encrypts a message with a key. Then the message receiver must decrypt the message with a key. Key families include: ▪ Symmetric. A symmetric key is where the sender uses a private key to encrypt a message. Then the recipient uses that same private key to decrypt it. ▪ Asymmetric. An asymmetric key is where the sender's key and receiver's key are different for the encryption and decryption processes. Key length is the number of bits used in a key by a cryptographic algorithm and can determine the strength.
Modes of Operation	Modes of operations include: ▪ Block Cipher: Provides confidentiality and authenticity services. A block cipher can encrypt or decrypt one fixed-length block. It encrypts or decrypts one large chunk of data (or block) at a time, often combining blocks for additional security. Block ciphers are more useful when the amount of data is known. ▪ Cipher Block Chaining (CBC): A plaintext block is combined with the previous cipher text block, and the result is encrypted with the key. ▪ Cipher Feedback (CFB): Each cipher text block is fed back into the encryption and then used to encrypt the next plaintext block. ▪ Output Feedback (OFB): The output blocks are fed back into the block cipher. These blocks then make strings of bits to feed the encryption algorithm, acting as the key generator. ▪ Counter (CTR): Both the sender and recipient access a reliable counter that computes a new shared value each time a ciphertext block is exchanged. The counter needs to be synchronized between both parties. ▪ Galois/Counter Mode (GCM): A variation of the Counter mode, GCM throughput rates do not require high performance hardware to produce acceptable high speed communication channels.
Output	The output from a cryptographic process may exhibit the following: ▪ A simple character change in the plaintext will cause several characters to change in the cipher text. This is called *diffusion*. ▪ When two different inputs to a cryptographic function produce the same output, this is called a *collision*. Collisions are not common, but can occur.
Digital Signature	A digital signature is a mathematical scheme for demonstrating the authenticity of digital message or document. A valid digital signature gives a message credibility, guaranteeing the recipient that the message has not been tampered with in transit.

Things to consider when choosing your cryptographic methods:

Concept	Definition
Low Power Devices	Some devices experience constraints on the amount of energy available to them. Some of these devices are wireless sensors, RFID tags, smart cards, mobile phones, and handheld tablets. These devices need to be secured using cryptography that provides fast identification, authentication and data protection. The issue is that low energy usage, while posing advantages in design and applicability, is also the cause of some security challenges because deploying security mechanisms and services consumes a large amount of power. While the processing power, memory, and network bandwidth of today's mobile devices are sufficient, battery power levels are increasing at a modest pace. These devices can still quickly drain their batteries. A security protocol running over these devices should utilize as little energy as possible. During a secure wireless session, the main sources of energy consumption are transmission and reception of packets, the overhead messages required for establishing the session, and cryptographic computations, in that order. One method to reduce energy consumption would be to select a combination of security primitives in a single session. Another way is to optimize the standard security protocols themselves. For example, wherever security needs are not that rigid, energy savings can be obtained by switching to smaller keys. Another way is to employ hardware acceleration of crypto-mechanisms. However, it can be difficult to provide customized hardware for encryption because this type of hardware is vulnerable to differential power analysis attacks.

Low Latency	*Latency* is the delay before a transfer of data begins to follow an instruction for its transfer. Lightweight ciphers are designed to be efficient based on size and power consumption. A new emphasis in lightweight ciphers is to achieve a lower latency (a lower response time). Automotive authentication systems and high-speed storage are examples of applications that require lower latency. Processing all rounds of the cipher in one clock cycle would achieve lower latency in a block cipher. This kind of implementation technique is called *round unrolling* or *unfolding*. In general, conventional block ciphers are implemented with a loop architecture, which processes one round of the cipher in one or a few clock cycles and repeats the process until the last round of the cipher.
High Resilience	High resilience cryptography (also know as leakage-resilient cryptography) refers to cryptographic protocols that remain secure and resistant to side channel attacks. Side channel attacks exploit devices that leak information to the outside world, not just through input-output interaction, but through physical characteristics like power consumption, timing, and electromagnetic radiation. This information leakage has been successfully used to break many cryptographic algorithms in common use. These leakages are particularly accessible when the device is at the hands of an attacker, as is often the case for modern devices, such as smart cards, mobile phones, and laptops. There are ongoing studies and research in leakage-resilient cryptography to tackle this challenge from an algorithmic angle. The idea behind the research is to design various cryptographic schemes that resist side channel attacks.
Supporting Confidentiality	Data encryption is a common method for ensuring confidentiality. Safeguarding data confidentiality involves training. Training should include strong passwords, user IDs, and multifactor authentication. Users can also take precautions to minimize the number of places where the information appears and the number of times it is actually transmitted to complete a required transaction. To prevent sensitive information from reaching the wrong people, access must be restricted to those authorized to view the data.
Supporting Integrity	Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire lifecycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people. These measures include cryptographic checksums for verification of integrity. Backups or redundancies must be available to restore the affected data to its correct state.
Supporting Obfuscation	Obfuscation is only secure if unwanted eyes don't know the mechanism used to camouflage the data. Obfuscation masks the data being sent. The goal is to camouflage the text making it incomprehensible to the interceptor unless the receiver knows the method use to obfuscate the text. If the receiver knows the method used, he can decipher the message. For example, instead of writing the text normally, you would: ▪ Reverse the order of the letters. ▪ Replace every plaintext letter with a different ciphertext letter. This is known as a substitution cipher. ▪ Replace a letter with a letter that is 13 places after it in the alphabet. This substitution cipher is known as ROT13, which is short for rotate 13. Since there are 26 characters in the alphabet, to undo the cipher, you apply the same ROT13 substitution. ▪ Perform an XOR (exclusive or) operation that combines the plaintext with a key. This is usually done at the bit level: 0 XOR 0 = 0, 0 XOR 1 = 1, 1 XOR 0 = 1, 1 XOR 1 = 0. The XOR operator is extremely common as a component in more complex ciphers.
Supporting Authentication	Multifactor authentication is one of the most cost effective mechanisms companies can use to protect digital assets. As more businesses move their servers into the cloud, better authentication is needed. With password breaches growing at an alarming rate, the need to improve authentication practices is undeniable. Deploying multifactor authentication forces people to use more than one authentication method, such as something you have along with something you know.
Supporting Non-Repudiation	*Non-repudiation* is the assurance that someone cannot deny something. It usually refers to ensuring that a party to a contract cannot deny the authenticity of their signature on a document or the sending of a message that they originated. A legal document may require witnesses so that the person who signs cannot deny having done so. With a digital signature, the idea is the same. You need to ensure that a message or document has been electronically signed by the correct person. Since no security technology is absolutely foolproof, some experts argue that a digital signature alone may not guarantee non-repudiation. It is suggested that multiple approaches be used, such as capturing unique biometric information and other data about the signer that would be difficult to repudiate collectively.
Resources vs. Security Constraints	The *Internet of Things* (IoT) is a network of physical resources, or devices, embedded with software, sensors, and connectivity that enables these devices to exchange data with the manufacturer and other connected devices. These devices are connected over the internet in the same way as laptops, tablets, smart phones, and Bluetooth devices are connected. Some of these devices can also remotely monitor or control home components, such as lighting and heating. Security protocols built on strong cryptographic algorithms use a pattern of analysis to defeat attacks, but these algorithms consume a lot of processor's efficiency. This is a security constraint because devices with limited capabilities, such as Internet of Things devices, need modified protocols that won't over-burden processors. The absence of strong security protocols may result in malicious attacks and malfunctions.