CHAPTER 6 — CRYPTOGRAPHY

6.1 GIVEn A SCENARIO, UTILIZE GENERAL CRYPTOGRAPHY CONCEPTS.

Symmetric vs. asymmetric

With symmetric key cryptography the sender and receiver of a message share a single common key. With asymmetric key cryptography there is one public key for encrypting messages and one private key for decrypting them.

Session keys

Session keys are single use, randomly generated symmetric keys for encrypting messages in a communication session.

In-band vs. out-of-band key exchange

With in-band exchange, key exchange takes place together with the communication process. With out-of-band exchange, key exchange takes place by some other means such as phone call, snail mail, face to face meeting ...etc.

Fundamental differences and encryption methods (Block vs. stream)

The two major types of encryption methods are Block Cipher and Stream Cipher. With the former, data is divided into blocks. With the latter, data is being operated on a bit by bit basis.

Transport encryption

With transport encryption, crypto services are applied to information which is above the network level and below the application level. There is no need to modify the application and the underlying networking services.

Non-repudiation

In order to enforce non-repudiation, a public key certificate to bind a public key with an identity should be used.

Hashing

Hashing is the act of using a hash function to take an arbitrary block of data and accordingly produce a fixed-size bit string (which is the cryptographic hash value).
Key escrow

A Key Escrow is a role necessary when a third-party needs access to encrypted data, such as when there is a court order to decrypt the encrypted data.

Steganography

Steganography means hiding information so that your data can become unreadable by a third party.

Digital signatures

Digital signature is a piece of data digest which is encrypted with the private key of the signer. It is always unique to the bearer.

Use of proven technologies

Use of proven technologies is important when dealing with cryptography. You should never use unproven technologies to secure your data!

Elliptic curve and quantum cryptography

Elliptic curve cryptography works based primarily on the algebraic structure of elliptic curves over finite fields. The elliptic curve Diffie–Hellman key agreement scheme is using the Diffie–Hellman scheme. Quantum cryptography, on the other hand, uses quantum mechanical effects to carry out cryptographic tasks.

Ephemeral key

A cryptographic key is considered as ephemeral when it is generated for each execution of the key establishment process. Sometimes it is possible for an ephemeral key to be utilized more than once within a single session.

Perfect forward secrecy

Perfect Forward Secrecy can ensure that a session key derived from a set of public and private keys will never get compromised even when one of the private keys is compromised. For this to work, the key that has been used to protect data transmission should not be utilized to derive additional keys.
6.2 Given a scenario, use appropriate cryptographic methods.

WEP vs. WPA/WPA2 and preshared key

WEP is not secure at all. WPA2 is more secure than WPA. A preshared key is a shared secret. This secret should have been shared between the parties using a secure channel. A key derivation function may be used to create such a secret.

MD5

Intended mainly for digital signature applications, MD5 uses a 128-bit hash value to create a hash which is typically a 32 character hex number.

SHA

Secure Hash Algorithm (SHA) refers to a set of cryptographic hash functions published by the NIST. SHA has several variants, including SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512. They are all designed by the NSA but published through the NIST.

RIPEMD

RACE Integrity Primitives Evaluation Message Digest (RIPEMD) is a suite of cryptographic hash functions developed basing upon MD4. Due to the weaknesses inherited, it has eventually been replaced by RIPEMD-128 and beyond.

AES

The Advanced Encryption Standard (AES) is established by the NIST. It is based on the Rijndael cipher. 3 different key lengths are supported, which are 128, 192 and 256 bits.

DES

Data Encryption Standard (DES) is a symmetric-key encryption method that uses a 56-bit key. Given today standard it is not so secure. See also 3DES.

3DES

3DES is a variation of DES which actually encrypts data for three times to enhance security. To be precise, 3 different 64-bit keys are used, which is supposed to be more secure.

HMAC

Keyed-hash message authentication code HMAC is a mechanism for message authentication using cryptographic hash functions to calculate a message authentication code. It first concatenates the key and the message and then get them hashed together.
RSA

RSA as a cryptosystem was one of the first practicable public-key cryptosystems for securing data transmission. With it, the encryption key is public while the decryption key needs to be kept secret.

Diffie–Hellman

Diffie–Hellman key exchange is a method for exchanging cryptographic keys. It allows two parties to jointly establish a shared secret key over an insecure channel. In fact, many Windows computers use it to create secure Internet Key Exchange IKE channel for IPsec based communications.

RC4

RC4 as the most widely used software stream cipher (it is used in TLS and WEP) is simple to use with good performance but security weaknesses are presented.

One-time pads (OTP)

One-time pads (OTB) refers to an encryption technique that is supposed to be non-crackable because a random secret key, which in never reused in whole or in part, is being utilized to perform encryption.

NTLM

NT LAN Manager (NTLM) refers to the MS security protocols for authentication, integrity, and confidentiality to Windows users. It works based on the mechanism of Windows Challenge/Response for authentication.

NTLMv2

NTLM V2 is a newer version of NTLM, introduced since Windows NT 4.0 SP4. It is now replaced by Kerberos in modern Windows Servers.

PGP/GPG

Pretty Good Privacy (PGP) is a popular technique for encrypting email messages sent over the internet (it can also send encrypted digital signature). The GNU Privacy Guard GPG is a free replacement for PGP.

TwoFish

Twofish is a symmetric key block cipher. It has a block size of 128 bits as well as a key size up to max 256 bits. It was published by Counterpane Labs back in 1998 and was an Advanced Encryption Standard AES finalist.

DHE

DHE (E means Ephemeral) uses normal diffie-hellman only.
ECDHE

ECDHE (EC means elliptic curve) uses elliptic curve diffie-hellman key exchange. There are known problems with it and there are suggestions saying that it may be better to switch back to DHE.

CHAP

Challenge Handshake Authentication Protocol (CHAP) does not ask for any password but instead deploys a challenge / response mechanism. MS CHAP is the MS implementation of CHAP. You find them primarily in Windows based network.

RADIUS

RADIUS is an access server and also a system of distributed security. It aims to secure remote access against unauthorized attempts. It can work with many other solutions to implement distributed security. Scalability is good.

PAP

Password Authentication Protocol (PAP) is an access control protocol for authenticating a user’s password. It works in clear text and is therefore not really secure.

Comparative strengths and performance of algorithms

When comparing methods for encryption techniques one must know the form of the input data to be operated on. As said before, the two major types are Block Cipher and Stream Cipher. With the former, data is divided into blocks. With the latter, data is being operated on a bit by bit basis. Generally, security is at the expense of performance.

Use of algorithms/protocols with transport encryption
(SSL, TLS, IPSec, SSH, HTTPS)

With transport encryption crypto, services are applied to information which is above the network level and below the application level. Secure Sockets Layer (SSL) is the predecessor of Transport Layer Security TLS. Both of them are cryptographic protocols that use X.509 certificates to perform asymmetric cryptography. IPSec, SSH and HTTPS are also for transport security.

Cipher suites
(Strong vs. weak ciphers)

Strong ciphers are cryptographically strong and are more resistant to cryptanalysis. Weak ciphers are the exact opposite.
Key stretching (PBKDF2, Bcrypt)

Key stretching refers to the act of making a weak key stronger and more secure against brute force attack. PBKDF2 short for Password-Based Key Derivation Function 2, which is a key derivation function for hashing passwords for storage. Bcrypt is a file encryption utility which is cross platform - the encrypted files are portable.

6.3 **GIVEN A SCENARIO, USE APPROPRIATE PKI, CERTIFICATE MANAGEMENT AND ASSOCIATED COMPONENTS.**

Certificate authorities and digital certificates (CA, CRLs, OCSP, CSR)

With a hierarchical trust model, there is a root CA and multiple subordinate CAs for providing redundancy and load balancing. With a Web of Trust cross-certification model, multiple CAs are in place to form peer-to-peer relationship. Online Certificate Status Protocol (OCSP) works by decoding revocation status requests for specific certificates and performing evaluation accordingly. You may use it as an alternative to or an extension of Certificate Revocation List CRLs for providing certificate revocation data to clients. A certificate signing request CSR is the message sent by an applicant to the CA to apply for a certificate.

**PKI**

A public-key infrastructure (PKI) is used to provide public key encryption and digital signature services. It includes hardware, software, the policies and the people involved.

**Recovery agent**

A Recovery Agent is a role allowed to decrypt a user’s data in case of emergency, such as when the original key is lost by the user.

**Public key**

The public key is for encrypting messages. When information transfer takes place from B to A, B can use A’s public key to encrypt the information.

**Private key**

The private key is for decrypting messages. When information transfer takes place from B to A, A will use his private key to decrypt the information encrypted by B.
Registration

In a PKI, the registration authority RA is in a role to ensure that the public key is bound to a particular individual to which it is assigned. In a Windows based network, a RA is usually a subordinate CA.

Key escrow

A Key Escrow is necessary when a third-party needs access to encrypted data, such as when there is a court order to decrypt the encrypted data.

Trust models

A PKI includes technologies, procedures and policies for propagating trust. How the actual trust propagation work is determined by the corresponding syntactic trust structure, which is the trust model.