Andrew Plum

Mr. Alves-Foss

Cyb 110

9/19/21

Ch. 5 Homework

1) A block cipher is a cryptographic algorithm that takes a predetermined number of bits known as a block and encrypts it using a cryptographic key. Typically, the length of the blocks in a block cipher are 64 bits. A stream cipher is a cryptographic algorithm which encrypts each bit separately. A block cipher can act as a stream cipher if its block size is set to one bit. Stream ciphers are fast whereas block ciphers are slow compared to stream ciphers. Stream ciphers have low error propagation due to each bit being encrypted at a time whereas block ciphers have high error propagation due to encrypting multiple bits in blocks. Block ciphers have high diffusion whereas stream ciphers have low diffusion. Most encryption algorithms in use are block ciphers.

2) Eve could do a man-in-the-middle attack in which she impersonates both Alice and Bob. She can trick Bob into believing that she is Alice by telling Bob she is Alice and then asking him for his Diffie-Hellman public key. Eve can then do the same with Alice. If she succeeds at tricking them that she is Alice or Bob and getting both their Diffie-Hellman public keys, she can then receive messages from Bob who believes Eve is Alice and then send the message, tampered or untampered, to Alice who believes Eve is Bob and vice-versa. This only works if Eve can trick both Alice into believing she is Bob and trick Bob into believing she is Alice.

3) There are several main differences between asymmetric and symmetric cryptography. The biggest difference between the two is in asymmetric cryptography there is a private key which is meant to be kept secret and a public key which is meant to be exchanged whereas in symmetric cryptography there is only a private key which is meant to be kept secret. In symmetric cryptography, data is encrypted and decrypted with the same key whereas in asymmetric cryptography, data is encrypted with private key and decrypted with public key and vice versa. Symmetric cryptography is used for confidentiality and integrity of data whereas public key cryptography can be used to provide confidentiality, integrity, and authenticity of data. Asymmetric cryptography is used to exchange keys. Symmetric cryptography is fast whereas asymmetric cryptography is slow compared to symmetric cryptography. These are some of the main differences between asymmetric and symmetric cryptography.

4) In electronic codebook mode, plaintext is taken and is encrypted using the key to get the ciphertext, and then the process is repeated using the same key on the next plaintext. Some advantages to electronic codebook are it is simple, fast, and it has support for parallel encryption and decryption. Some disadvantages to electronic codebook are duplicate data in plaintext is repeated in ciphertext, plaintext can be changed by changing the ciphertext, and it can't resist replay attacks. In cipher block chaining mode, the first ciphertext is created by having the first plaintext exclusive-or with the initialization vector (every time hereafter this process is repeated, the plaintext exclusive-or's with the previously encrypted ciphertext) and then being encrypted by the key, and the process is repeated for each subsequent block in the chain. Some advantages of cipher block chaining are it has support for parallel decryption, you can decrypt any ciphertext packet, and duplicate data in plaintext is not repeated in ciphertext. Some disadvantages of cipher block chaining are it does not support parallel

encryption and corrupted blocks in the chain will affect subsequent blocks in the chain. In cipher feedback mode, the ciphertext is created by encrypting the initialization vector with the key and exclusive-or'ing the result with the plaintext, and then every subsequent ciphertext is created using the same process except instead of the initialization vector being encrypted with the key, the previous ciphertext is encrypted with the key. Some advantages of cipher feedback are no padding is needed, it has support for parallel decryption, it can decrypt any ciphertext packet, and it can prepare keys for encryption and decryption. Some disadvantages of cipher feedback are it does not support parallel encryption, it can't resist replay attacks, and corrupted blocks will affect subsequent blocks.

5) The best way to avoid having a software that falls prey to these hidden assumptions and other errors is implement asymmetric cryptography because it clears up hidden assumptions and other errors that break many "cryptographic key exchange" protocols. Because of the nature of asymmetric cryptography, authenticity of the data is provided. Digital signatures which use hash functions allow you to see whether or not a sent message was altered, and public-key certificates allow you to verify that a public key is truly associated with an individual. The downside of asymmetric cryptography is that it is much slower than symmetric cryptography.