Quiz 5

CSE-644 INTERNET SECURITY

DR. SYED SHAZLI

2/22/2023

Anthony Redamonti
SYRACUSE UNIVERSITY

1) What is secret-key Encryption, is it secure enough and why, or why not?

Secret-key encryption is the process of using one key to encrypt and decrypt data. It is not secure as anyone with the secret-key can decrypt the entire message or encrypt a new message. It is easier to decode the secret-key if it is symmetric (used for both encryption and decryption).

2) What is mono and poly alphabetic substitute cipher? What is the famous example for poly? Why is it hard to decode?

Monoalphabetic Substitution Cipher = only one substitution cipher (one permutation). Each letter in the original message is passed through the same cipher for encryption.

Polyalphabetic Substitution Cipher = each letter uses a different substitution table (permutation). The positioning of the letter determines which substitution table is applied to it.

The famous example of a polyalphabetic substitution cipher is the enigma machine using by Germany in WWII. It is difficult to decode because there were 3 rotors from sets of five, each having 26 different positions, yielding a total of 158,962,555,217,826,360,000 (158 quintillion) different settings.

3) What is DES? How does it work(briefly)? What is AES? Why is AES better?

The data encryption standard (DES) was a symmetric encryption key algorithm introduced to the public domain in 1977. It encrypted digital data in sections of 64-bit blocks. Each 64-bit block is sent through a 56-bit encryption key, and what is output is the encrypted data. Because it used a 56-bit encryption key, it is too unsecure to be used by modern applications.

The advanced encryption standard (AES) is a block cipher that uses a variable key length of either 128, 192, or 256 bits. It encrypts 128-bit blocks of memory by performing four operations multiple times (rounds): substitution of bytes, shifting of rows, mixing of columns (matrix multiplication), and use of round keys (the output of the column mixing is XOR-ed with the key).

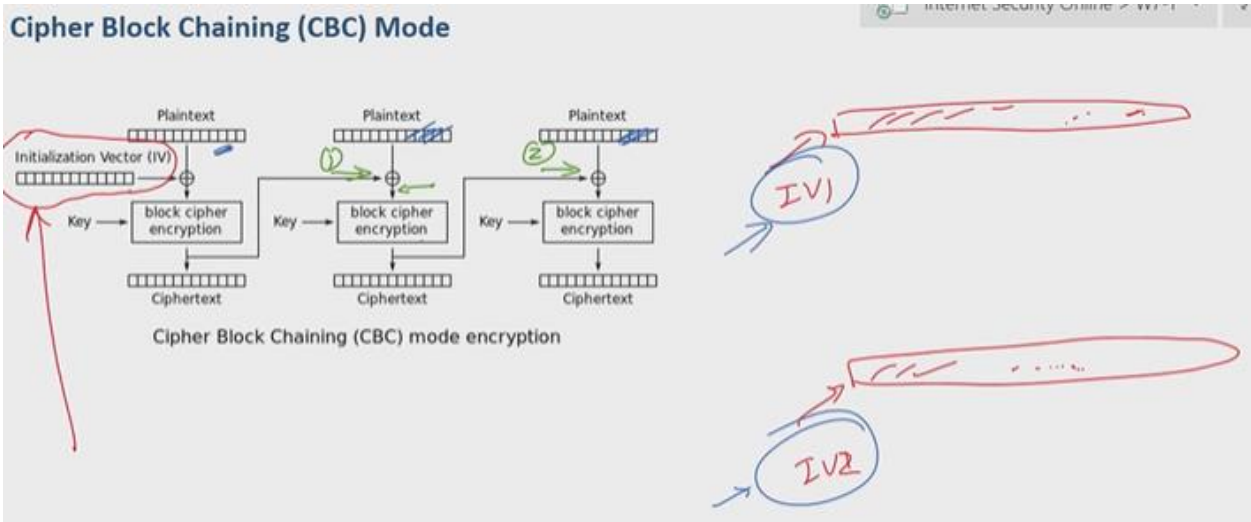
AES is better because it is a more involved process of encryption. It utilizes a four-step process instead of a single step. The AES algorithm has been implemented directly inside modern CPU's and has never been broken.

4) What are those Encryption modes discussed in the book and lectures? Brief explain the encryption method for each mode ECB, CBC, CFB and OFB and if you change one bit in second block of encrypted file, when you decode it, how many and which blocks stay the same and how many and which blocks get corrupted?

Electronic Code Book (ECB) mode encryption uses a key fed into an AES encryption algorithm to encrypt blocks of data. If one bit in the second block of the encrypted file is corrupted, then only that block is corrupted. The corruption does not bleed into the next block.

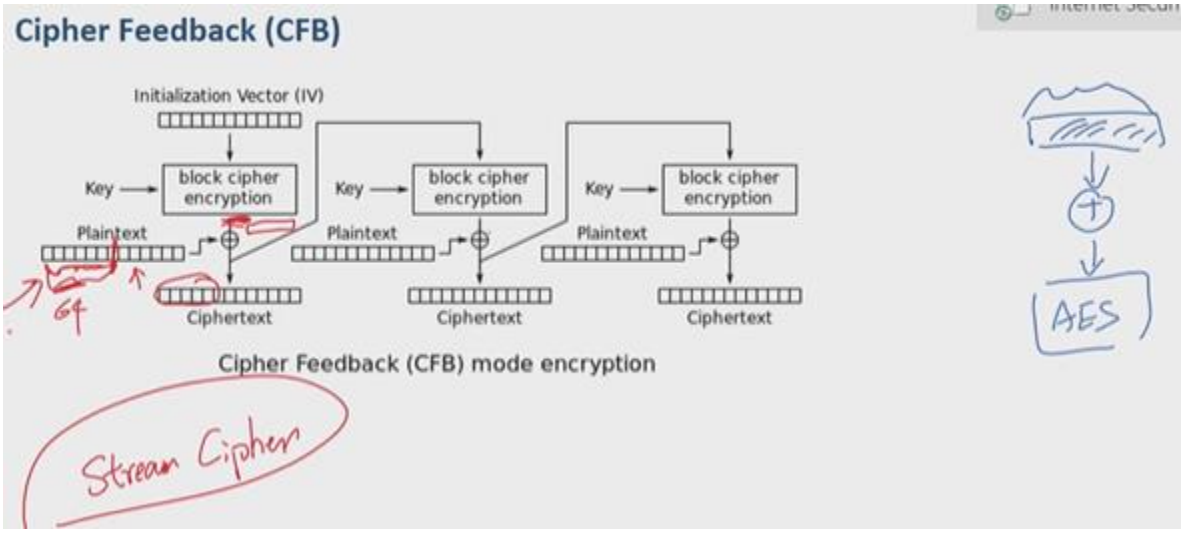
Cipher Block Chaining (CBC) mode encryption uses an initialization vector that is XOR-ed with the plaintext. The output of the XOR operation is fed into a block cipher encryption algorithm, and the output is the ciphertext. The ciphertext is then used in the XOR operator in the next block of encryption.

If one bit from the second block of ciphertext is corrupted, during decryption the entire second block will be corrupted along with one bit of the next block.



Cipher Feedback (CFB) mode encryption uses an initialization vector and a key that are fed into a block cipher encryption algorithm. The output of that algorithm is XOR-ed with the plaintext to generate the ciphertext. The ciphertext and the key are fed into the block cipher encryption algorithm for the encryption of the next block.

If one bit from the second block of ciphertext is corrupted, during decryption the entire second block will be corrupted.



Output Feedback (OFB) mode encryption algorithm works almost the same way as the CFB except for one important difference: the output of the block cipher encryption is used as the input to the next

block cipher encryption algorithm BEFORE being XOR-ed with the plaintext. By changing the order of operations, all the encryption happens in parallel instead of sequentially.

If one bit from the second block of ciphertext is corrupted, during decryption the entire second block will be corrupted.