CRYPTOGRAPHY HOMEWORK-1 REPORT

Q1-) Stream ciphers are ciphers which encrypt a digital data one bit or one byte at time. Keystreams should be provided to both users via some secure independent channel, which can be very hard if data traffic is very large. A block ciphers are ciphers in which a block of plaintext is treated as bulk and used to produce ciphertext block in equal length. Typical block sizes used are 64-bit or 128-bits. Stream ciphers are often used for their speed and simplicity of implementation in hardware, and in secure wireless connection where plaintext comes in unknown length. As an example of block cipher, AES can be used for security in SSL(Secure Socket Layer) and in TLS(Transport Layer Security) internet connections to government data. For instance NSA (National Security Agency) relies on the AES encryption to secure its data which is categorized up to top secret.

Q2-) In CBC mode of operation initialization vector is generated randomly but it is actually public , so when it has to be sent to receiver it should be encrypted with mode usually like ECB (electronic code book). According to properties of XOR operation we can state:

$$\neg P[i] = \neg IV[i] \oplus D(K,C_i)[i]$$

where negation notation denotes bit complementation. Above notation indicates that if an opponent can change bits in IV the corresponding bits of the received value P_i can be changed. So thats why it can be more protective to send IV after encrypting it with ECB.

Q3-) Security of CBC is moderate in general , but especially if an attacker captures or somehow able to change the any ciphertext at any point, then all ciphertexts that come after it will also be corrupted which is a weakness for CBC mode of operation. Compared to ECB it is still a better mode because in ECB it may be possible for cryptanalyst to capture some regularities if the message contains repeating structures, so by collecting many plaintext-ciphertext pairs, cryptanalyst can start to figure out the key. Also there are some other new modes that can be worked with AES such as cipher feedback (CFB), output feedback(OFB), and CTR(counter) mode. Some of these

modes can be used to convert block ciphers into stream ciphers. In some some of these mode as each character can be encrypted and transmitted at the same time they provide real-time operations. CFB mode is similar to CBC but at each encryption phase leasts significant s bits of the shift register is replaced by previous step's ciphertext, so even if ciphertext is corrupted at any stage, corrupted part can be discarded by many shifts and select operations in shift registers. In OFB mode each encrypted data block is independent of plaintext and output of this encryption is given as feedback to next encryption phase, thus even if ciphertext is corrupted at any stage this that corruption will not be propagated to subsequent phases. Weakness of OFB is that it tends to message stream modification attacks because complementing the bits in ciphertext complements the corresponding bits in plaintext. So changes changes can be done to plaintext by just changing bits in ciphertext. CTR mode uses a unique counter value for each encryption which can also be done in parallel to increase the performance. Another advantage of CTR mode is that it allows random access to ith plaintext block which can be useful in applications that needs to decrypt just single block. As only encryption algorithm is needed and decryption key scheduling need not to be implemented , it is faster than other mode of of operations in general.

REFERENCES

- Cryptography and Network Security Principles and Practice Global Edition, William Stallings(pg.213,pg.216,pg.218,pg.220) Chapter 7 Block Cipher Operation.
- **www.Informit.com** Understanding Application Layer Protocols Article.
- **https://en.wikipedia.org/wiki/Block_cipher** Block Cipher
- **https://en.wikipedia.org/wiki/Stream_cipher** Stream cipher