Unit – 02: Mathematics of cryptography

- DES Block ciphers modes and Feistel ciphers DES.
- working of DES,
- cracking des, problems on des.
- 2DES, 3DES, des design,
- Side channel attacks,
- Differential cryptanalysis.

Questions to be discussed:

1. Discuss the term DES. Write the applications of DES Algorithm.
2. Explain different DES Modes of Operation.
3. Differentiate between DES and AES algorithms.
4. Discuss about 2DES and 3DES in brief.
5. What is a side-channel attack?

Mathematics of cryptography:

- Mathematics of cryptography means use of mathematical techniques to encode plain text with hash functions and perform crypto-analysis to identify the original text from encrypted keys.

Difference between Symmetric and Asymmetric Key Encryption:

Symmetric Key Encryption	Asymmetric Key Encryption
It only requires a single key for both encryption and decryption.	It requires two keys, a public key and a private key, one to encrypt and the other one to decrypt.
The size of cipher text is the same or smaller than the original plain text.	The size of cipher text is the same or larger than the original plain text.
The encryption process is very fast.	The encryption process is slow.
It is used when a large amount of data is required to transfer.	It is used to transfer small amounts of data.
It only provides confidentiality.	It provides confidentiality, authenticity, and non-repudiation.
The length of key used is 128 or 256 bits	The length of key used is 2048 or higher
Examples: 3DES, AES, DES and RC4	Examples: Diffie-Hellman, ECC, DSA and RSA

Data Encryption Standard (DES)

- DES stands for Data Encryption Standard.
- DES is a Symmetric Key Encryption technique.
- DES is based on the Feistel block cipher, called LUCIFER.
- It was developed in 1971 by IBM cryptography researcher Horst Feistel.
- The DES algorithm uses a key of 56-bit size.
- Using this key, the DES takes a block of 64-bit plain text as input and generates 64-bit cipher text block.
- The DES process has several steps involved in it, where each step is called a round.
- DES's dominance came to an end in 2002, when the Advanced Encryption Standard replaced the DES.
- It was adopted in 1977 for government agencies to protect sensitive data & was officially retired in 2005.
- The Triple DES (3DES), remains approved for sensitive government information through 2030.

Applications of DES Algorithm:

Some of the applications of the DES Algorithm.

1. It is used in random number generation
2. It is deployed when not-so-strong encryption is needed
3. It is used to develop a new form of DES, called Triple DES (using a 168-bit key formed using three keys)

Different DES Modes of Operation:

DES have five different modes of operation:

1. Electronic Codebook (ECB).
2. Cipher Block Chaining (CBC).
3. Cipher Feedback (CFB).
4. Output Feedback (OFB).
5. Counter (CTR).

ECB:

- ECB stands for Electronic Codebook.
- Each 64-bit block is encrypted and decrypted independently.

CBC:

- CBC stands for Cipher Block Chaining.
- Each 64-bit block depends on the previous one and uses an Initialization Vector (IV).

CFB:

- CFB stands for Cipher Feedback.
- The preceding ciphertext becomes the input for the encryption algorithm, producing pseudo random output, which in turn is XORed with plaintext, building the next ciphertext unit

OFB:

- OFB stands for Output Feedback.
- Much like CFB, except that the encryption algorithm input is the output from the preceding DES.

Counter (CTR):

- CTR stands for Counter.
- Each plaintext block is XORed with an encrypted counter.
- The counter is then incremented for each subsequent block

Difference between DES and AES algorithms:

DES	AES
Used to encrypt plain text of 64-bit	Used to encrypt plain text of 128-bit
The key is of 56-bit size.	The key is of different sizes such as 128-bits, 192-bits, and so on
Less secure than AES	More secure than DES
It can be broken by brute force attacks	To date, AES has not been attacked
It is based on Feistel network	It is based on permutation and substitution network

Working of DES:

- As we know that DES is a Symmetric Key Encryption technique.
- So, it uses the same key to encrypt and decrypt a message.
- Both the sender and the receiver must know and use the same private key.
- Some key features affecting how DES works include the following:

Block cipher:

- The Data Encryption Standard is a block cipher, meaning a cryptographic key and algorithm are applied to a block of data simultaneously rather than one bit at a time.
- To encrypt a plaintext message, DES groups it into 64-bit blocks.
- Each block is enciphered using the secret key into a 64-bit cipher text by means of permutation and substitution.

Several rounds of encryption:

- The DES process involves encrypting 16 times.
- It can run in four different modes, encrypting blocks individually or making each cipher block dependent on all the previous blocks.
- Decryption is simply the inverse of encryption, following the same steps but reversing the order in which the keys are applied.

64-bit key:

- DES uses a 64-bit key, but because eight of those bits are used for parity checks, the effective key length is only 56 bits.
- The encryption algorithm generates 16 different 48-bit sub keys, one for each of the 16 encryption rounds.
- Sub keys are generated by selecting and permuting parts of the key as defined by the DES algorithm.

Replacement and permutation.

- The algorithm defines sequences of replacement and permutation that the cipher text undergoes during the encryption process.

Backward compatibility.

- DES also provides this capability in some instances.

Cracking DES:

- In cryptography, the DES cracker is a machine built by the Electronic Frontier Foundation in 1998.
- It is used to perform a brute force search to decrypt an encrypted message by trying every possible key.
- The aim in doing this was to prove that the key size of DES was not sufficient to be secure.
- It is also known as EFF DES cracker or "Deep Crack".
- Detailed technical data of this machine, including block diagrams, circuit schematics have all been published in the book Cracking DES.
- Its public domain license allows everyone to freely copy, use, or modify its design.

What are the drawbacks of DES? Problems on DES?

The drawbacks include the following:

- The 56-bit key size of the DES algorithm is arguably its worst drawback.
- A million DES operations may be encrypted and decrypted by chips in a second.
- For $1 million, you may get a DES cracking machine that will search all the keys in around seven hours.
- What is the main weakness of DES?
- Probably the biggest disadvantage of the DES algorithm is the key size of 56-bit.
- There are chips available that can encrypt and decrypt a million DES operations in a second.
- A DES cracking machine that can search all the keys in about seven hours is available for $1 million.

2DES and 3DES:

- As we know that DES uses 56 bit key to encrypt any plain text which can be easily be cracked by using modern technologies.
- To prevent this from happening double DES and triple DES were introduced which are much more secured than the original DES because it uses 112 and 168 bit keys respectively.
- They offer much more security than DES.

Double DES:

- Double DES is an encryption technique which uses two instance of DES on same plain text.
- In both instances it uses different keys to encrypt the plain text.
- Both keys are required at the time of decryption.
- The 64 bit plain text goes into first DES instance which then converted into a 64 bit middle text using the first key and then it goes to second DES instance which gives 64 bit cipher text by using second key.
- However double DES uses 112 bit key but gives security level of 2^56 not 2^112 and this is because of meet-in-the middle attack which can be used to break through double DES.

Triple DES:

- Triple DES is an encryption technique which uses three instance of DES on same plain text.
- It uses there different types of key choosing technique in first all used keys are different and in second two keys are same and one is different and in third all keys are same.
- Triple DES is also vulnerable to meet-in-the middle attack because of which it give total security level of 2^112 instead of using 168 bit of key.
- The block collision attack can also be done because of short block size and using same key to encrypt large size of text.
- It is also vulnerable to sweet32 attack.

What is a side-channel attack?

- A side-channel attack does not target a program or its code directly.
- It attempts to gather information of a system by measuring indirect effects of the system.
- SCA is a security exploit that attempts to extract secrets from a chip or a system.
- This can be achieved by measuring or analyzing various physical parameters.
- **Examples** include supply current, execution time, and electromagnetic emission.

Differential Cryptanalysis:

- It is used to find the "difference" between related plaintexts that are encrypted.
- The plaintexts may differ by a few bits.
- It is usually launched as an adaptive chosen plaintext attack: the attacker chooses the plaintext to be encrypted (but does not know the key), and then encrypts related plaintexts.
- The cryptanalyst then uses statistical analysis to search for signs of non-randomness in the cipher texts, zeroing in on areas where the plaintexts differed.
- Every bit of the related cipher texts should have a 50/50 chance of flipping: the cryptanalyst searches for areas where this is not true.
- Any such underlying order is a clue to recover the key.