**DEALINE:** To be submitted through the class rep latest Monday 19th October, 2020 at 5.00 p.m

**BCT 2314 – ASSIGNMENT**

1. Explain the working mechanisms of the below block ciphers

a) Serpent (10 marks)

* Serpen**t** is a [symmetric key](https://simple.wikipedia.org/wiki/Symmetric-key_algorithm) [block cipher](https://simple.wikipedia.org/wiki/Block_cipher)
* Serpent has a [block size](https://simple.wikipedia.org/wiki/Block_size_(cryptography)) of 128 bits and supports a [key size](https://simple.wikipedia.org/wiki/Key_size) of 128, 192 or 256 bits.
* The [cipher](https://simple.wikipedia.org/wiki/Cipher) is a 32-round [substitution-permutation network](https://simple.wikipedia.org/wiki/Substitution-permutation_network) operating on a block of four 32-bit words
* Each round applies one of eight 4-bit by 4-bit S-boxes32 times in parallel.
* Serpent was designed so that all operations can be executed in parallel using 32 1-bit slices.
* This maximizes parallelism, but also allows use of the extensive cryptanalysis work performed on DES

b) IDEA (10 marks)

It is a symmetric key block ciphers that:

* uses a fixed-length plaintext of 16 bits and
* encrypts them in 4 chunks of 4 bits each
* to produce 16 bits cipher text.
* The length of the key used is 32 bits.
* The key is also divided into 8 blocks of 4 bits each.

This algorithm involves a series of 4 identical complete rounds and 1 half-round. Each complete round involves a series of 14 steps that includes operations like:

* Bitwise XOR
* Addition modulo
* Multiplication modulo

After 4 complete rounds, the final “half-round” consists of only first 4 out of the 14 steps previously used in the full-rounds. To perform these rounds, each binary notation must be converted to its equivalent decimal notation, perform the operation and the result obtained should be converted back to the binary representation for the final result of that particular step.

**Key Schedule:** 6 subkeys of 4 bits out of the 8 subkeys are used in each complete round, while 4 are used in the half-round. So, 4.5 rounds require 28 subkeys. The given key, ‘K’, directly gives the first 8 subkeys. By rotating the main key left by 6 bits between each group of 8, further groups of 8 subkeys are created, implying less than one rotation per round for the key (3 rotations).

c) CAST (10 marks)

* CAST ciphers are [Feistel ciphers](https://en.citizendium.org/wiki/Feistel_cipher) using large S-boxes, 8\*32 rather than the 6\*4 of DES. They are primarily designed for software implementation, rather than the 1970s hardware DES was designed for, so looking up a full computer word at a time makes sense. An 8\*32 S-box takes one K byte of storage; several can be used on a modern machine without difficulty.
* They take 32-bit words from several S-boxes and combine them to form a 32-bit output, so that the **F** function has ideal avalanche properties — every output bit depends on all S-box output words, and therefore on all input bits and all key bits
* The CAST S-boxes use [bent functions](https://en.citizendium.org/wiki/Bent_function) (the most highly nonlinear Boolean functions) as their columns. That is, the mapping from all the input bits to any single output bit is a bent function. Such S-boxes meet the strictavalanche criterion ; not only does every every bit of round input and every bit of round key affect every bit of round output, but complementing any input bit has exactly a 50% chance of changing any given output bit. Bent functions are combined to get additional desirable traits — a balanced S-box (equal probability of 0 and 1 output), minimum correlation among output bits, and high overall S-box nonlinearity.

**CAST-128**,

* Also called CAST5, is the best-known and most widely used CAST cipher.
* CAST-128 is a Feistel cipher with 64-bit blocks and 16 rounds. Key sizes from 40 to 128 bits are supported; 128 is almost invariably used. There are eight 8\*32 S-boxes, four used in the key schedule and the other four in actual encryption. Round keys are 37 bits.
* The F function XORs the input with 32 bits of round key, splits the result into bytes and runs each byte through a different S-box to get four 32-bit results. Those are combined nonlinearly, using different combining functions in different rounds. Finally, the output is given a rotation controlled by the other 5 round key bits.

**CAST 256**

* It uses 128-bit blocks and supports key sizes of 128, 192 or 256 bits.
* It is a variant of [Feistel cipher](https://en.citizendium.org/wiki/Feistel_cipher) using four 32-bit sub-blocks. In the terms of the [MARS](https://en.citizendium.org/wiki/MARS_(cipher)) team, it is a "Type 1 Feistel network"; each round takes one 32-bit block as input and alters one block. 48 rounds are used. The round function and S-boxes are identical to CAST-128.

**BCT 2314 - CAT**

1. What requirements must a public-key cryptosystems fulfill to be a secure algorithm? (4 marks)

* It is computationally infeasible for an adversary, knowing the public key, and cipher text to recover the original message.
* It is computationally infeasible for an adversary knowing the public key to determine the private key.
* It is computationally easy for a party B to generate a pair of keys(Pub,Prb)
* It is computationally easy for a sender A, knowing the public key and message to be encrypted to generate corresponding cipher text.(C=E(Pub,M)

1. Outline the components of the RSA algorithm (4 marks)

* Plaintext: readable message that is fed into the algorithm as input.
* Encryption algorithm: performs various transformations on the plaintext.
* Public and Private keys: Exact transformations performed by the algorithm depend on the public and private key provided as input.
* Ciphertext: Scrambled message produced as output. Depends on the plaintext and key for a given message. 2 different keys will produce 2 different cipher texts.

1. Let (𝑃𝑈𝑎,𝑃𝑅𝑎) be the public and private key of Alice, and (𝑃𝑈𝑏,𝑃𝑅𝑏) are the public and private key of Bob. Let ( ) be a hash function, (𝐾𝑒𝑦,𝐷𝑎𝑡𝑎) denote an encryption, and 𝐷(𝐾𝑒𝑦,𝐷𝑎𝑡𝑎) decryption operation, || denotes a concatenation and 𝐷𝑜𝑐 be a document. Describe the digital signature algorithm performed by Alice, on the document 𝐷𝑜𝑐. (5 marks)
   * Alice generates two keys, (𝑃𝑈𝑎,𝑃𝑅𝑎)
   * She keeps the private and sends the public to Bob.
   * After creating the message (Doc), she generates a digest by hashing the memo using the hash function ( ).
   * She then encrypts the digest with her private key, ,𝑅𝑎. The encrypted digest is the signature for the message.
   * Alice now sends the memo and digital signature to Bob.
2. Let (𝐾𝑒𝑦,𝑀) denote a message authentication code function, produced for the message M and a shared key Key. Let (𝐾𝑒𝑦,𝑀) denote encryption of a message M with a key Key, and let || denote the concatenation. If Alice send to Bob the following information: (𝐾2,𝑀)||𝐶(𝐾1,𝐸(𝐾2,𝑀)) where 𝐾1,𝐾2 are shared secret keys. Describe the goals of the message. (4 marks)

* The shared secret keys are used to generate the key Key which enables decryption and encryption of a message by either party.
* Authentication. This gives the receiver (Bob), reason to believe that the message created and sent by Alice.
* Non-repudiation. Ensures that the sender (Alice can’t deny having sent the message later on.
* Integrity. Gives the assurance that the message wasn’t changed in transit.

1. In the Diffie Hellman Key exchange protocol between user A and B both users have a private key: 𝑋𝐴=6 and 𝑋𝐵=35, respectively. The public keys are 𝑌𝐴=𝑎𝑋𝐴 𝑚𝑜𝑑 𝑝 and 𝑌𝐵=𝑎𝑋𝐵 𝑚𝑜𝑑 𝑝. What is the common key K for p = 71 and a = 7? (4 marks)

STEP 1

Alice:

Alice uses her private key to calculate

7^6 mod 71=2

She shares this result with Bob.

Bob

Bob uses his private key to calculate

7^35 mod 71=23.

He shares his result with Alice.

STEP 2

Alice takes Bobs result and raises it to the power of her private number:

23^6 mod 17=8

Bob takes Alice’s result and raises it to the power of his private number:

2^35 mod 17 =8

Common key is 8.

.

6. The RSA system was used to encrypt the message M into the cipher-text C = 6. The public key is given by 𝑛=𝑝.𝑞=187 and 𝑒=107. By answering the following, try to crack the system and to determine the original message M.

a. What parameters comprise the public key and the private key? (2 marks)

* Pub(n,e)
* Pr(d)

b. What steps are necessary to determine the private key from the public key? (2 marks)

* Private Key d is calculated from p, q, e. For a given n and e,there is a unique number d.
* Number d is the inverse of e modulo (p-1) (q-1). This means that d is the number less than (p-1) (q-1) Such that when multiplied by e, it is equal to 1 modulo (p-1) (q-1).
* The relationship:de=1 mod(p-1)(q-1)

c. Determine the private key for the given system. (5 marks)

pq=187; e=107;

187 is a product of two primes. The only possibilities are 17, 11.

(p-1)(q-1)=16.10 or 10.16=160.

d.e=1 mod 160.

d.170=1 mod 160.

Extended Euclidian Algorithm;

160(x) +107(y)=1

(160,107)160=107.1+53

(107, 53)107=53.2+1

(53, 1)53=53.1+0

Solve for remainders;

53=160-107.1

1=107-53.2.

Substitute 1=107-53.2

For 53;

107-(160-107)2

107-(160.2-107.2)

107-160.2+107.2

107.3-160.2

d=3

d. What is the original message M? (2marks)

C^d mod n=M

6^3 mod 187

Ans: 108

7. Recall the ElGamal cryptosystem. A community of users share a large prime p and a primitive element a. Each user has a key pair (𝑥,), where 0<𝑥<𝑝−1 is randomly chosen and 𝑌=𝑎𝑥 𝑚𝑜𝑑 𝑝. Y is public and x is private. To send a message M to Alice, who has key pair (𝑥𝐴,𝐴), Bob performs the following steps:

i. Choose a random 𝑥𝐵 with 0<𝑥𝐵 <𝑝−1.

ii. Compute 𝐶1=𝑎𝑥𝐵 𝑚𝑜𝑑 𝑝 and 𝐶2=𝑀.𝐴𝑥𝐵 𝑚𝑜𝑑 𝑝

iii. The ciphertext is (𝐶1,2).

1. Explain how Alice decrypts the message, show the steps. (5 marks)

* The result of C1 is sent to Alice so that she can compute the secret shared key.
* She will take Bobs result (C1) and raise it to the power of her private number 𝑥𝐴 so as to obtain the shared key;C1^ 𝑥𝐴 mod p.
* Now that she has the shared key, she can obtain message M; C2=M. C1^ 𝑥𝐴 mod p.

M=C2/ C1^ 𝑥𝐴 mod p

1. Assume that prime p = 17 and the primitive element a = 6. Bob, who has a private key 𝑥𝐵=12 wants to send a message M = 5 to Alice, who has a public key 𝑌𝐴=15. Compute the ciphertext is (𝐶1, 2). and show your steps. (5 marks)

𝐶1=𝑎𝑥𝐵 𝑚𝑜𝑑 𝑝

𝐶1=6^12 mod 17

=13

Bob shares this result with Alice.

He now computes the private shared key using Alice’s result(15)

15^12 mod 17=16

𝐶2=𝑀.𝐴𝑥𝐵 𝑚𝑜𝑑 𝑝

=5.16

=80

9. A Feistel cipher is used in the DES algorithm.

a. Describe the operation of a Feistel cipher. (5 marks)

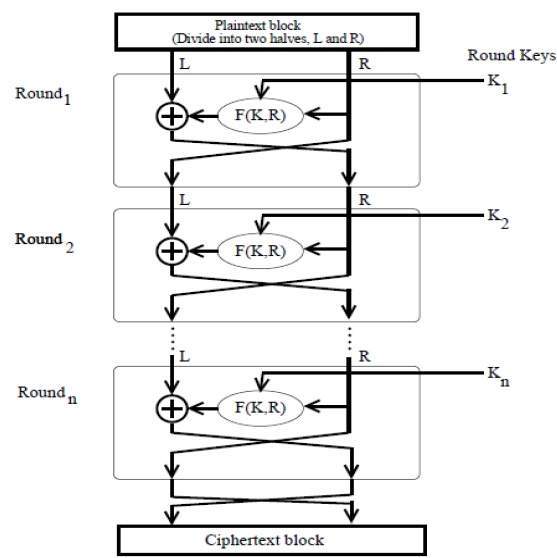
It is essentially a kind of framework of building encryption algorithm.

It is a structure, then you put in some encryption rounds and keys and then it turns it into a cipher for you. y

**Encryption Process**

The encryption process uses the Feistel structure consisting multiple rounds of processing of the plaintext, each round consisting of a “substitution” step followed by a permutation step.

Feistel Structure is shown in the following illustration − you.bbb



* The input block to each round is divided into two halves that can be denoted as L and R for the left half and the right half.
* In each round, the right half of the block, R, goes through unchanged. But the left half, L, goes through an operation that depends on R and the encryption key. First, we apply an encrypting function ‘f’ that takes two input − the key K and R. The function produces the output f(R, K). Then, we XOR the output of the mathematical function with L.
* In real implementation of the Feistel Cipher, such as DES, instead of using the whole encryption key during each round, a round-dependent key (a subkey) is derived from the encryption key. This means that each round uses a different key, although all these subkeys are related to the original key.
* The permutation step at the end of each round swaps the modified L and unmodified R. Therefore, the L for the next round would be R of the current round. And R for the next round be the output L of the current round.
* Above substitution and permutation steps form a ‘round’. The numbers of rounds are specified by the algorithm design.
* Once the last round is completed then the two sub blocks, ‘R’ and ‘L’ are concatenated in this order to form the ciphertext block.

The difficult part of designing a Feistel Cipher is selection of round function ‘f’. In order to be unbreakable scheme, this function needs to have several important properties that are beyond the scope of our discussion.

**Decryption Process**

The process of decryption in Feistel cipher is almost similar. Instead of starting with a block of plaintext, the ciphertext block is fed into the start of the Feistel structure and then the process thereafter is exactly the same as described in the given illustration.

The process is said to be almost similar and not exactly same. In the case of decryption, the only difference is that the subkeys used in encryption are used in the reverse order.

The final swapping of ‘L’ and ‘R’ in last step of the Feistel Cipher is essential. If these are not swapped then the resulting ciphertext could not be decrypted using the same algorithm.

b. Briefly describe three modes of operation of DES. (5 marks)

* Cipher block chaining: it is a mode of operation for block cipher in which a sequence of bits are encrypted as a single unit or block with a cipher key applied to the entire block.
* Electronic CodeBook Mode; A mode of operation for a block cipher, with the characteristic that each possible block of plain text has a defined corresponding ciphertext value and vice versa.
* Output Feedback Mode: Mode of operation that makes a block cipher into a synchronous stream cipher. It generates keystream blocks, which are then XORed with plaintext blocks to get the ciphertext.