**BCT 2314 – ASSIGNMENT**

**Name: STANLEY NGUGI Registration Number: SCT212-0065/2017**

1. **Explain the working mechanisms of the below block ciphers**
2. **Serpent (10 marks)**

Serpent has a block size of 128 bits and supports a key size of 128, 192 or 256 bits. The cipher is a 32-round substitution-permutation network operating on a block of four 32-bit words. Each round applies one of eight 4-bit by 4-bit S-boxes 32 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.

1. **IDEA (10 marks)**

It is a symmetric key block cipher 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).

1. **CAST (10 marks)**

* CAST ciphers are Feistel ciphers 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 (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 strict avalanche criterion; not only does 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 using four 32-bit sub-blocks. In the terms of the MARS 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.