Applied Cryptography, Monsoon 2022
Homework 1

This is a programming assignment. You can choose to do any three of the five given questions. However it is mandatory to implement at least one question that is based on block ciphers and one based on stream ciphers. Your submission should be a zip file containing the implementation files. All questions carry the same marks.

1. Advanced Encryption Scheme (AES) is one of the two National Institute of Standards and Technology (NIST) approved block cipher schemes. Depending on the length of the key used, there are three variants of AES — AES-128, AES-196 and AES-256. Implement the AES encryption and decryption scheme. The encryption algorithm should take as inputs a bit string message of size 128 bits, a security parameter $l \in \{128, 196, 256\}$ and a key of length l to output the ciphertext. The decryption algorithm should similarly take as input a ciphertext of size 128 bits, a security parameter $l \in \{128, 196, 256\}$ and a key of length l to output the plaintext.

2. Data Encryption Scheme (DES) is one of the earliest block cipher schemes. However, due to its short key size of 56 bits, DES has been shown to be insecure against the modern computers. To overcome this shortcoming, NIST recommends the use of Triple DES which believed to be practically secure. Implement Triple DES encryption and decryption functions. The inputs to the encryption (decryption) function should be a tuple of three keys of length 56 bits and plaintext (ciphertext) and the output of the function should be the 128 bit ciphertext (plaintext).

3. Recall that Trivium is one of the finalist ciphers in the eSTREAM stream cipher project in the hardware profile. You can find the specifications of Trivium here

   (a) Implement Trivium cipher. The function should take as input an 80 bit key, 80 bit IV and a parameter l such that $1 \leq l \leq 2^{15}$ to output an l length bit stream generated via Trivium.

   (b) Show some evidence that the period of Trivium is at least 2^{30}. (Note that doing it for merely a single key does not suffice but you might not be able to show the same for all possible keys. You might have to take some large enough set of randomly chosen keys and show that the period of the stream is not less than 2^{30} for each key.)

4. TRIAD is one of the Round 1 candidates of the Lightweight Cryptography Project by NIST. The specifications of the cipher can be found here. Construct a function that implements the encryption and decryption algorithms of TRIAD-AE cipher. The encryption functions should take as input a key K, nonce N and a message M and output a ciphertext C. The decryption function should take as input a key K, nonce N and the ciphertext C. (You can ignore the generation of tag using `TriadMAC` and hence need not take an associated data A as input in any of the functions.

5. Consider the cipher in Figure 1. The SPN consists of 4 rounds. Baring the last round, each round of this SPN consists of (i) key mixing, (ii) substitution, and (iii) permutation. The last round of the SPN consists of key mixing, substitution which is again followed by key mixing. For any i^{th} round, the round key κ_i is obtained from the original key $K = k_1 k_2 \cdots k_{16}$ as $\kappa_i = K \ll_r (11 * i)$ for $i \in \{1, 2, 3, 4, 5\}$ where $a \ll_r b$ denotes left circular shift of the bits of a by b positions. The action of the S-box function on inputs is as given in Table 1. As for the permutation, the i^{th} output bit after the substitution layer is the $P(i)^{th}$ input bit to the next round where $P()$ is as defined in Table 2.

input	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
output	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

Table 1: Representation of S-box

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
P(i)	1	9	17	25	2	10	18	26	3	11	19	27	4	12	20	28
i	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
P(i)	5	13	21	29	6	14	22	30	7	15	23	31	8	16	24	32

Table 2: Permutation

(a) Implement the SPN. The function should take as input a message M of length 32 bits and key K of length 32 bits and output a ciphertext C of length 32 bits encrypted through this SPN.

(b) Construct a linear approximation trail on this SPN such that in any round at most 1 S-box is active and for any S-box, the input and output masks have at most 1 bit set to 1.

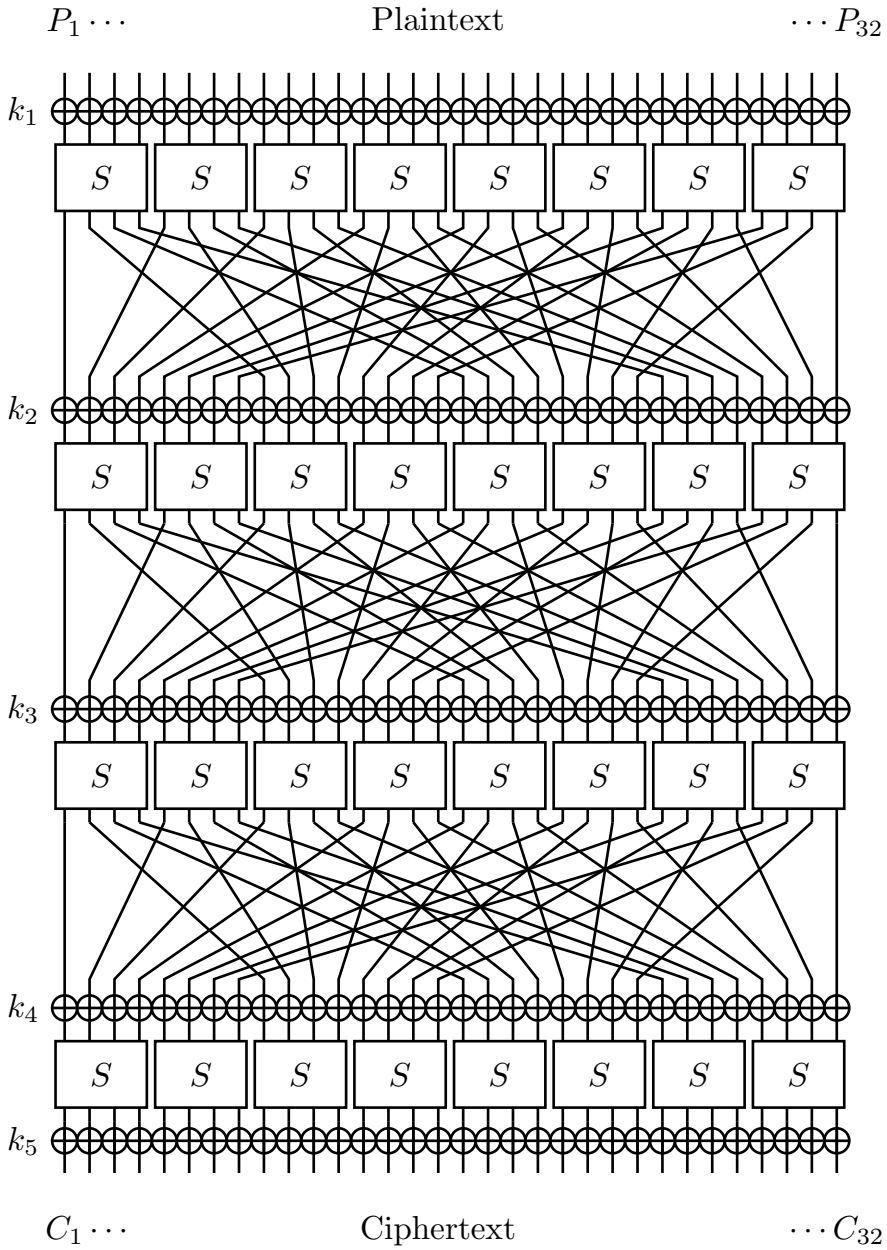

Figure 1: A Toy SPN Cipher