Prof. Dr. Berna Örs Yalcın **Due Date:** 07 May 2021

BLG520E Cryptography
2nd Project

1. Build three different block ciphers with the following properties

   (a) They are substitution-permutation networks (SPNs) with 16-bit block length.

   (b) They include four rounds.

   (c) The key schedules for all the block ciphers is performed by using a 16-bit linear feedback shift register (LFSR) [2] as shown in Eq. 1 and 2.
   Master key: $K_0 = [k_{0,15}\, k_{0,14}\, k_{0,13}\, k_{0,12}\, k_{0,11}\, k_{0,10}\, k_{0,9}\, k_{0,8}\, k_{0,7}\, k_{0,6}\, k_{0,5}\, k_{0,4}\, k_{0,3}\, k_{0,2},\, k_{0,1}\, k_{0,0}]$
   i-th round key:

$$k_{i,15} = k_{i-1,0} \oplus k_{i-1,2} \oplus k_{i-1,4} \oplus k_{i-1,5} \quad (1)$$
$$k_{i,j} = k_{i-1,j+1} \quad (2)$$

Block Cipher 1:

SBox:

z	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\pi_S(z)$	1	9	6	D	7	3	5	F	2	C	E	A	4	B	8	0

Permutation:

z	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
$\pi_P(z)$	15	11	7	3	14	10	6	2	13	9	5	1	12	8	4	0

Block Cipher 2: SBox: $\pi_S(z) = \begin{cases} 0 & if \quad z = 0 \\ z^{-1} \bmod 17 & if \quad 1 \le z \le 15 \end{cases}$,

SBox:

z	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\pi_S(z)$	0	1	9	6	D	7	3	5	F	2	C	E	A	4	B	8

Permutation:

z	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
$\pi_P(z)$	15	11	7	3	14	10	6	2	13	9	5	1	12	8	4	0

Block Cipher 3: SBox: $\pi_S(z) = \begin{cases} 0 & if \quad z = 0 \\ z^{-1} \bmod 17 & if \quad 1 \le z \le 15 \end{cases}$,

SBox:

z	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\pi_S(z)$	0	1	9	6	D	7	3	5	F	2	C	E	A	4	B	8

Permutation:

z	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
$\pi_P(z)$	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

2. Choose a random key. Produce some random or chosen plaintext, ciphertext pairs for all the three different block ciphers.

3. Sedat İn, Süleyman Eser, Fikret Başar Gencer, Ceyhun Yamaneren, Nur Elif Topuz, Ali Üstün, Muhammed Mustafa Öney, Fahri Anıl Yerlikaya,Muhammet Cevher Kavan, Muhammed Güneş, Abdulsamet Eraslan, Mümin Göker Gayretli, Yakup Hüner, Yusuf Okutan will apply linear cryptanalysis [5, 1, 3] to above block ciphers.

4. Recep Onur Yıldız, Metin Akkın, Umut Çoltu, Ayşe Sayın, Doğancan Davutoğlu, Burak Eruluğ, Raşit Rıdvan Turgut, Gizemnur Taşkın, Sevgi Nur Bilgin, Fidan Bozkurt, Fatih Öner, Sertaç Karadeniz, Alişan Aygar, Nida Fidan will apply differential cryptanalysis [4, 3] to above block ciphers.

5. Compare and discuss the results for all the block ciphers.

References

[1] Alex Biryukov and Christophe De Cannière. *Linear Cryptanalysis for Block Ciphers*, pages 351–354. Springer US, Boston, MA, 2005.

[2] S. Gaonkar. Design of 8 bit, 16 bit and 32 bit lfsr for pn sequence generation using VHDL. *International Journal of Technical Research and Applications*, 31:305–308, 2015. e-ISSN: 2320-8163.

[3] H. M. Heys. *A Tutorial on Linear and Differential Cryptanalysis.*

[4] X. Lai, J.L. Massey, and S. Murphy. Markov ciphers and differential cryptanalysis. In D. W. Davies, editor, *Advances in Cryptology: Proceedings of EUROCRYPT'91*, volume 547 of *Lecture Notes in Computer Science*, pages 17– 38, Brighton, UK, April 1991. Springer-Verlag.

[5] M. Matsui. Linear cryptanalysis method for DES cipher. In T. Helleseth, editor, *Advances in Cryptology: Proceedings of EUROCRYPT'93*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397, Lofthus, Norway, May 23-27 1993. Springer-Verlag.