COL 759

Tutorial Sheet 4

Due Date: 28^{th} Jun 2020

1. A binary sequence which satisfies Golomb′s randomness postulates is called a pseudo-noise sequence or a pn-sequence. Consider the periodic sequence s = 011001000111101 of period n =15. Is this sequence pn-sequence? Justify your answer.

2. The so called S-box (Substitution box) is widely used cryptographic primitive in symmetric-key cryptosystems. In AES (Advanced Encryption Standard) the 16 S-boxes in each round are identical. All these S-boxes implement the inverse function in the Galois Field GF(2^8), which can also be seen as a mapping, S : $\{0, 1\}^8 \to \{0, 1\}^8$, so that

   $$x \in GF(2^8) \to x^{-1} \in GF(2^8)$$

   i.e. that is 8 input bits are mapped to 8 output bits. What is the total number of possible mappings one can specify for function S?

3. In cryptography and computer security, man-in-the-middle attack (MITM), is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other.
   (i) Describe how a man-in-the-middle attack may be performed on a Wi-Fi network and the consequences of such an attack.
   (ii) Explain how a man-in-the-middle attack on a Wi-Fi network can be defeated.

4. Consider a plaintext of size 1024 bits, has a probability of 0.7 for producing a 0 and the LFSR sequence has about 60% 0's. Find the approximate number of 0's in the resulting cipher.

5. Show that any m-sequence is G-random.

6. Prove that out-of- phase autocorrelation function of an m-sequence with period $2^n - 1$ is $\frac{-1}{2^n-1}$.

7. Suppose we wish to construct an m-sequence of length 31. Using polynomial 45 (in octal). Write the resulting m-sequence by LFSR with initial sequence (1, 0, 0, 0, 0).

8. Let s be a periodic binary sequence with period p. Let k be the number of entries 1 in one period of s and μ is the number of pairs $(s_i, s_{i+\tau}) = (1, 1)$ for a fixed $\tau < p$, $0 \leq i \leq p$. Then prove that the autocorrelation coefficients $C(\tau)$ is

$$C(\tau) = 1 - \frac{4(k - \mu)}{p}$$

9. An affine block cipher is one where the key specifies a non-singular 3 by 3 matrix **A** and an 3-tuple **t** to define the affine transformation **c** = **Am** + **t** where , **m** is a block of plaintext (size *s*) and **c** is the corresponding ciphertext. **c**, **A** and **m** all are over GF(2). Find the number of affine block ciphers.

10. Each of the following points has finite order on the given elliptic curve over Q. In each case, find the order of P.
(a) $P = (0, 16)$ on $y^2 = x^3 + 256$
(b) $P = (1/2, 1/2)$ on $y^2 = x^3 + (1/4)x$
(c) $P = (3, 8)$ on $y^2 = x^3 - 43x + 166$
(d) $P = (0, 0)$ on $y^2 + y = x^3 - x^2$

11. Consider elliptic curve over F_{2^4} (field of characteristic 2) is

$$E: y^2 + xy = x^3 + g^4x^2 + 1,$$

where $g = (0010)$ is generator of F_{2^4}. F_{2^4} is constructed using primitive polynomial $f(x) = x^4 + x + 1$. List all the elements in $E(F_{2^4})$.