Problem set I

Virendra Sule

August 26, 2020

(*Note*: This is a set of problems and questions relevant to exploring basic questions on symmetric key Cryptography. Problems and question in test and exam shall be of similar nature except may be with lesser lengthy answers than required for the present set).

1. Construct as many examples of One Way (OWF) and Trapdoor One Way Functions (TOWF). A mathematical representation of the these is

$$\begin{array}{lrcl} \text{OWF} & y & = & F(x) \\ \text{TOWF} & y & = & F(k,x) \text{ Trapdoor } k \end{array}$$

The input x, output y and trapdoor (key) k are strings over alphabets or just symbols. Properties required to be satisfied by F for OWF and TOWF are discussed in the Introductory notes. The examples should give a relative difficulty and ease of computation in the definition of these functions. (A mechanical analogy of a TOWF is a box with a lock which has two keys. Message x is put in the box by sender and the box is locked. The locked box is denoted by y. The box is delivered to the sender by a trusted courier who does the job of delivering the box faithfully. The receiver has the same key exchanged a priori. It is relatively much difficult to open the box without opening the lock). Which of the following can be considered TOWFs justify giving mathematical arguments.

   (a) p is large size prime. $y = x^k \mod p$.

   (b) p is large size prime. $y = k^x \mod p$.

   (c) p is large size prime. $y = (x+k)^{-1} \mod p$. The number $x + k \neq 0 \mod p$. For any number $a \neq 0 \mod p$ the inverse b can be found such that $ab = 1 \mod p$.

   (d) $y = k_1x_1 + k_2x_2 + k_3 \mod p$.

   (e) How will you build TOWFs using Vigenere, Diana and Rotor ciphers which may be practically useful?

   Largeness of prime in these problems refers to difficulty of computation in relation to the length of the prime (number of bits in its binary expansion).

2. A substitution cipher is defined by substituting alphabets uniquely to other alphabets. A transposition cipher is defined by permuting the positions of alphabets in the plaintext. How will you recognise whether a ciphertext is created by substitution or transposition?

3. If a plaintext stream is given as input to the three rotor cipher and ciphertext collected from other two rotors alternatively, how will you break this cipher to find plaintext from ciphertext?

4. Develop computational tests to measure the relative OWF and TOWF properties. You can assume that X, Y and K are finite sets defined by strings of bits or finite fields of integers modulo a prime number. Given $F(x)$ or $F(k, x)$ construct computational conditions to define and how to test, computing y given x is easy and computing x given y is difficult. Similarly for the conditions of the TOWF.

5. Think of ways in which you can exchange the key k securely. Banks still exchange the initial (random) PIN numbers of your account login or card securely by creating the sealed double paper slip in a machine. You dont accept an unsealed slip.

6. Suppose $y = F(x)$ is a relatively practical OWF. How can you construct a TOWF using F?

7. If $y = F(k, x)$ is a practical TOWF. If you construct a new TOWF as follows,

$$z = G((k_1, k_2), x) = F(k_2, F(k_1, x))$$

Is G stronger TOWF (more secure) than F? Justify. Let $y = E(k, x)$ be an encryption function whose decryption function is $x = D(k, y)$. Is the function

$$y = E(k_1, D(k_2, E(k_1, x)))$$

stronger TOWF than E?

8. Construct the TOWF as in the above problem for using E defined by TWOFs of examples in problem 1.

9. Fibbonacci sequences modulo a number. A sequence of numbers a_n for $n = 1, 2, \ldots$ generated by the recurrence $a_n = a_{n-1} + a_{n-2}$ and initial condition $a_1 = a_2 = 1$ is called a Fibonacci sequence. The sequence grows very fast to large numbers hence we can define Fibonacci sequences modulo a number N. Construct Fibonacci sequences modulo primes $N = 3, 5, 7, 19, 31, 43$ defined by recurrence

$$a_n = a_{n-1} + a_{n-2} \mod N$$

with $a_1 = a_2 = 1$. Prove that such sequences are ultimately periodic for any initial condition, i.e. there exits m and a period r such that $a_{n+r} = a_n$ for $n > m$. For an arbitrary initial condition a_1 and a_2 in numbers modulo N, find the period r of the sequence.

10. Determine the linear complexities of the sequences generated by following stream ciphers for different initial loading of registers. Find the periods of these sequences if they are periodic and the index m after which the sequence is periodic.

    (a) $L[1, 0, 1, 0]$ with sequence defined by the output function $y(k) = x_1(k) \oplus x_2(k)x_3(k)$.

    (b) Two LFSRs with an output sequence. $L1[1, 1, 0, 1]$, $L2[1, 0, 0, 1]$ with outputs y_1, y_2 respectively (the leftmost bit). The output sequence defined by $y = y_1 \oplus y_2 \oplus y_1y_2$.

    (c) Two LFSRs as $L1$, $L2$ of previous problem with $L3[1, 0, 1, 1]$ with output y_3. Output sequence defined by MSB of the integer $y = y_1 + y_2 + y_3$ (the integer sum of three outputs).

    (d) FSR defined by $L[1, 1, 0, 1]$ with recurrence rule $x_4 = \text{MSB}\,(x_0+x_1+x_3)$ which is the ingteger sum.

11. Consider an encryption function $y = E(k, x)$ defined by $y = x^k \mod p$ where the symmetric key is $0 < k \leq p-1$ and the gcd $(k, p-1) = 1$ i.e. k has no common factor with $p-1$. Then show that the decryption function is $x = D(l, y)$ defined by $x = y^l \mod p$ such that $kl = 1 \mod p - 1$.

    (a) Verify the encryption decryption formulas for different primes p.

    (b) For a prime p let the set of alphabets be $[0, p - 1]$. Consider the encryption function E as a block cipher with block length 1 (single alphabet) denoted as $(a1)(a2)\ldots(am)$. For different cases of p, plaintexts P, ciphertexts C, keys k, modes of operations indicated in the table below find the missing items.

p	P	C	k	Mode	IV,X_0
37	(10)(2)(4)(11)	?	15	CBC	2
11	?	(10)(9)(8)(7)	3	CBC	3
31	(21)(7)(9)(11)	?	7	CTR	2
57	?	(2)(11)(3)(3)	3	CTR	2

12. Consider the stream cipher of problem 8(b). Assume the key $K = (1, 0, 1, 1)$ as the initial state of $L1$ and $IV = (1, 1, 0, 1)$ the initial state of $L2$. Let the key stream be chosen from $k_0 = 8$. Encryption is as $c_i = p_i \oplus k_{k_0+i}$ for $i = 0, 1, 2, \ldots$. Decrypt the sequence $1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1$.