CSD451- Applied Cryptography

Assignment-2

Max marks:25
Submit by Sat. 30/09/23, 23.59 17-Sept-2023

1. Consider each of the the following encryption schemes and prove whether the scheme is perfectly secure or not. You can provide a counterexample in case the scheme is not perfectly secure.

   (i) Let n be a positive integer. A Latin square of order n is an $n \times n$ array L of the integers $1, \ldots, n$ such that every one of the n integers occurs exactly once in each row and each column of L. An example of a Latin square of order 3 is as follows:

1	2	3
3	1	2
2	3	1

   Given any Latin square L of order n, we can define a related Latin Square Cryptosystem. Take $\mathcal{M} = \mathcal{C} = \mathcal{K} = 1, \ldots, n$. For $1 \leq i \leq n$, the encryption rule Enc is defined to be $Enc_i(j) = L(i, j)$. (Hence each row of L gives rise to one encryption rule.) Give a complete proof that this Latin Square Cryptosystem achieves perfect secrecy provided that every key is used with equal probability. [5]

   (ii) A variable length one-time pad Π is defined as having keys of some fixed length L while messages and ciphertexts are variable length bit-strings of length at most L(including the empty string) i.e., $\mathcal{K} = \{0,1\}^L$ and $\mathcal{M} = \mathcal{C} = \{0,1\}^{\leq L}$ for some parameter L. The encryption for $k \in \{0,1\}^L$ and message $m \in \{0,1\}^{\leq L}$ of length l is defined as

   $$Enc_k(m) = k[0, \ldots, l-1] \oplus m$$

   and for a key $k \in \{0,1\}^L$ and a ciphertext $c \in \{0,1\}^{\leq L}$ of length l, the decryption function is defined as:

   $$Dec_k(c) = k[0, \ldots, l-1] \oplus c$$

   Verify if correctness property holds for Π? Proof that the above cipher is not perfectly secure. [5]

   (iii) Suppose the 26 keys in the Shift Cipher are used with equal probability 1/26. Then prove that for any plaintext probability distribution, the Shift Cipher has perfect secrecy.

   [5]

2. Suppose you are told that the one time pad encryption of the message "attack at dawn" is "$09e1c5f70a65ac519458e7e53f36$" (the plaintext letters are encoded as 8-bit ASCII and the given ciphertext is written in hex). What would be the one time pad encryption of the message "attack at dusk" under the same OTP key? [5]

3. Suppose an algorithm G is a pseudorandom generator. Let G' be the following algorithm: on input seed s, run $G(s)$ to get w, then negate every bit of w to get w' (i.e., for bit i, $w_i{}' = 1 - w_i$), and output the result. Prove that G' is also a pseudorandom generator. [5]