CS304: Introduction to Cryptography & Network Security

Assignment II

Course Instructor: Dr. Dibyendu Roy Due: May 01, 2024, 11:59 pm

Instructions: Clearly write your name and roll number on the top of each page. Solutions must be handwritten. I expect all students to behave according to the highest ethical standards. Any cheating or dishonesty of any nature will result in deduction of marks. Your submission will not be considered if you submit through email.

1. The DES S-box S_4 has some unusual properties:
   (a) Prove that the second row of S_4 can be obtained from the first row by means of the following mapping:
   $$(y_1, y_2, y_3, y_4) \to (y_2, y_1, y_4, y_3) \oplus (0, 1, 1, 0)$$
   where the entries are represented as binary strings.
   (b) Show that any row of S_4 can be transformed into any other row by a similar type of operation.

2. Describe in detail how both encryption and decryption in CTR mode can be parallelized efficiently.

3. Suppose that $X = (x_1, \ldots, x_n)$ and $X' = (x'_1, \ldots, x'_n)$ are two sequences of n plaintext blocks. Suppose X and X' are encrypted in OFB mode using the same key and the same IV. Show that it is easy for an adversary to compute $X \oplus X'$. Show that a similar result holds for CTR mode if ctr is reused.

4. Construct two LFSRs using the following two connection polynomials and find their periods.
   (a) $f(x) = x^4 + x + 1$.
   (b) $f(x) = x^5 + 1$.

5. Suppose $\lambda : \mathbb{Z}_{105} \to \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7$ is defined as
   $$\lambda(x) = (x \mod 3, x \mod 5, x \mod 7).$$
   Give an explicit formula for the function λ^{-1} and use it to compute $\lambda^{-1}(2, 2, 3)$.

6. Solve the following system of congruences:
   $$\begin{aligned} x &\equiv 12 \mod 25 \\ x &\equiv 9 \mod 26 \\ x &\equiv 23 \mod 27. \end{aligned}$$

7. In RSA cryptosystem consider $n = 18923$ and the encryption key $e = 1261$. For the ciphertext $c = 6127$ find the corresponding plaintext. Explain each and every step.

8. Let EL be the elliptic curve $y^2 = x^3 + 5x + 3$ defined over $\mathbb{Z}_{13}$. Find out all the possible points on EL. Provide justification against your answer.

9. Suppose that we use the SPN presented in Example 4.1 of Stinson's book, but the S-box is replaced by a function π_T that is not a permutation. This means, in particular, that π_T is not surjective. Use this fact to derive a ciphertext-only attack that can be used to determine the key bits in the last round, given a sufficient number of ciphertexts that all have been encrypted using the same key.

10. Consider the hash function $h : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ defined by $h(x, y) = (ax + by) \mod n$, where $a, b \in \mathbb{Z}_n$ and $n \geq 2$. Prove that if you know hashed value corresponding to two inputs then you can find the hashed value of many inputs without applying hash function on those inputs.

11. Let p be a prime number For $a, b \in \mathbb{Z}_p$, define $f(a, b) : \mathbb{Z}_p \to \mathbb{Z}_p$ by the rule $f_{(a,b)}(x) = ax + b \mod p$. Let $x \neq x' \in \mathbb{Z}_p$ such that $f_{(a,b)}(x) = y$ and $f_{(a,b)}(x') = y'$. Given x, x', y, y' is it possible to find $a, b \in \mathbb{Z}_p$, if possible derive a, b, if not give proper justifications.