2^{nd} Class Test on

Cryptography and Network Security (CS60065)

Duration: 1 hour Time: 12 noon Date: 9.11.2022

Full Marks - 20

Answer All the Questions

1. (a) Write down the Wiener's attack Theorem.
   (b) Compute the continued fraction expansion of 35/99 by applying the Euclidean Algorithm.
   (c) Also derive the convergents of the above continued fraction.

[1+1.5+2.5]

2. (a) Let g be a primitive root for Fp. Suppose that $x = a$ and $x = b$ are both integer solutions to the congruence $g^x \equiv h \pmod p$. Prove that $a \equiv b \pmod{p-1}$.
   (b) Suppose that $p > 2$ is prime and $\alpha \in \mathbb{Z}_p^*$. Then prove that α is a primitive element modulo p if and only if $\alpha^{(p-1)/q} \not\equiv 1 \pmod p$ for all primes q such that $q|(p-1)$.
   (c) Calculate the time complexity of Pollard p-1 algorithm.

[2+2+1]

3. (a) After having studied the Diffie-Hellman protocol, a young cryptographer decides to implement it. In order to simplify the implementation, he decides to use the additive group $(\mathbb{Z}_p, +)$ instead of the multiplicative one $(\mathbb{Z}_p^*, .)$. As an experienced cryptographer, what do you think about this new protocol?

   (b) Suppose Bob has an RSA Cryptosystem with a large modulus n for which the factorization can't be found, e.g., n is 1024 bits long and Alice sends a message to Bob by representing each alphabetic character as an integer between 0 and 25 (i.e., $A \to 0$, $B \to 1$, . . . $Z \to 25$) and then encrypting each letter as a separate plaintext character. Describe how an eavesdropper can easily decrypt a message which is encrypted in this way.

[2+3]

4. Consider the Diffie-Hellman key exchange procedure between Alice and Bob. Alice selects a large prime number p and a multiplicative generator g (mod p). Both p and g are made public. Alice picks a secret random x, with $1 \le x \le (p-2)$. She sends $M_A = g^x \pmod p$ to Bob. Bob picks a secret random y, with $1 \le y \le (p-2)$. He sends $M_B = g^y \pmod p$ to Alice. Using the received messages, Bob and Alice compute the shared session key K.

   Suppose Eve discovers that $p = Tq + 1$, where q is an integer and T is small. Eve intercepts M_A and M_B sent by Alice and Bob respectively. Eve sends Bob $M_A^q \pmod p$, and sends Alice [redacted] $M_B^q \pmod p$.

   (a) Show that Alice and Bob calculate the same shared key K′.
   (b) Show that there are only T possible values for K′, so Eve may find K′ by exhaustive search.

[2+3]