Introduction to Information Security (H1)

Quiz-2 (Spring 2024)
International Institute of Information Technology, Hyderabad
Time: 1 Hour and 20 Minutes Total Marks: 40
Instructions: Answer ALL questions.
This is an open notes examination.
No query is allowed in the examination.
Use of Regular Calculator is allowed.

15 Feb 2024

1. (a) In the RSA-based public key cryptosystem, suppose you are given $p = 19$, $q = 23$ and $e = 3$. Find n, $\phi(n)$ and d.

   (b) Suppose you want to implement RSA algorithm using the following encoding procedure:
   A = 01, B = 02, $\cdots$, Z = 26, , = 27, . = 28, ? = 29, 0 = 30, 1 = 31, ..., 9 = 39, ! = 40 (the blank space is considered as 00).
   Let the plaintext you have taken as *Cryptography is an interesting subject!* Assume that the lower and upper case letters have the same encoding values. For exaple, C and c have the same numerical value 03.

   (i) Encode the plaintext using the given encoding standard.

   (ii) Assume that the public key of Bob supplied to you as $(e, n) = (7, 187)$. Determine the number of plaintext blocks.

   (iii) Encrypt the third plaintext block using the RSA encryption.

   [6 + 3 + 2 + 7 = 18]

2. Parties A and B decide upon the prime $p = 101$ and the primitive root $\alpha = 3$ for using the Diffie-Hellman key exchange protocol in order to establish a secret session key between them. Suppose the party A picks $X_A = 70$ and party B picks $X_B = 87$ as their private keys. Compute the session key between A and B. By detailed calculation, show that they both do indeed arrive at the same value.

   [12]

3. Let two parties A and B agree on the following digital signature scheme. Entity A signs a binary message m of arbitrary length. Entity B can verify this signature by using the public key of A.

   Entity A performs the following steps in key generation:
   (i) Select two primes p and q such that $q \mid (p-1)$.
   (ii) Select a random integer g with $1 < g < p-1$, such that $\alpha = g^{(p-1)/q} (\mathrm{mod} p)$ and $\alpha > 1$.
   (iii) Select a private key a, $1 \leq a \leq q-1$.
   (iv) Compute $y = \alpha^a (\mathrm{mod} p)$.
   Public key of A is (p, q, α, y).

   After key generation, A generates the signature on m the message as follows:
   (i) Select a random secret integer k, $1 \leq k \leq q-1$.
   (ii) Compute $r = \alpha^k \bmod p$, $e = H(m||r)$, and $s = (a.e - k) \bmod q$, where $H(\cdot)$ is a one-way hash function.
   (iii) Select two random secret integers u and v, $0 < u < q$ and $0 < v < q$, and compute $r' = r\alpha^{-u} y^v \bmod p$.
   (iv) Compute $e' = H(m||r')$ such that $e' = e + v$ and $s' = s + u$.
   A then sends the signed message $(m, (e', s'))$ to the verifier B.

   Devise a verification algorithm for the party B. Prove the verification equation mathematically.

   [6 + 4 = 10]

********** End of Question Paper **********