Indian Institute of Technology, Kharagpur

Date...................... Time: 60 mins Full Marks: 25
Third Class Test (Autumn) Semester 2020-21 No. of Students: 56
Sub. No. MA 61027 Subject Name: Cryptography and Network Security

Instruction: The test is in open-book, open-notes mode. Answer all questions. No marks will be awarded without proper justification. Notations used are as explained in the class.

1. [$2 + 2 = 4$ **mark**] Here is a variation of the ElGamal Signature scheme. The key is constructed in a similar manner as before: Alice chooses a generator g of ${Z_p}^\star$ and a random integer a, $0 \leq a \leq p-2$, such that $\mathsf{gcd}(a, p-1) = 1$, and computes $g^a \bmod p$. Alice's public key is $(p, g, g^a \bmod p)$ and her private key is a. Let $m \in {Z_p}^\star$ be a message to be signed. Alice computes the signature (r, s) on message m, where

$$r = g^k \mod p,$$

$$s = (h(m) - kr)a^{-1} \mod (p-1).$$

Here h is a suitable hash function. The only difference from the original ElGamal Signature Scheme is the computation of s. Answer the following questions concerning this modified scheme:

   (a) Describe how a signature (r, s) on a message m would be verified using Alice's public key.

   (b) Describe computational advantage of the modified scheme over the original scheme.

2. [$2 + 2 = 4$ **mark**]

   (a) Determine the Galois field $\mathsf{GF}(3^3)$ generated by $x^3 + 2x + 1 = 0$ and list down the polynomial equivalents for each ternary 3-tuple in this field.

   (b) Find the inverse of 121 in $\mathsf{GF}(3^3)$ generated by $x^3 + 2x + 1 = 0$.

3. [$1 + 2 = 3$ **mark**] The field $\mathsf{GF}(2^5)$ can be constructed as $\mathbb{Z}_2[x]/(x^5 + x^2 + 1)$.

   (a) Compute $(x^4 + x^2) \times (x^3 + x + 1)$.

   (b) Using the **Extended Euclidean algorithm**, compute $(x^3 + x^2)^{-1}$.

4. [2 **mark**] Show that the Decisional Diffie-Hellman (DDH) problem is not hard in the multiplicative group Z_p, for any odd prime p.

5. [$3+3 = 6$ **mark**] Let E be the modular elliptic curve defined by $y^2 = x^3 + 3x \pmod{17}$.

   (a) Find all points of E (including the point at infinity).

   (b) Find $2(8, 14)$.

——-P.T.O.———

6. [3 **mark**] Let $\mathcal{G}$ be a Bilinear Diffie-Hellman (BDH) instance generator, i.e., $\mathcal{G}$ on input a security parameter k outputs (q, G_1, G_2, e, P) where q is prime, G_1, G_2 are groups of order q, $e : G_1 \times G_1 \rightarrow G_2$ an admissible symmetric bilinear pairing and P a generator of G_1. Show that if the Computational Diffie-Hellman (CDH) problem in G_2 is easy, then the BDH problem with respect to $\mathcal{G}$ is easy.

7. [3 **mark**] Let $e : G_1 \times G_1 \rightarrow G_2$ be a symmetric admissible bilinear pairing, where both G_1 and G_2 are prime order groups of order q. For a fixed but arbitrary $Q \in G_1^*$ define the isomorphism $f_Q : G_1 \rightarrow G_2$ by $f_Q(P) = e(P, Q)$. Show that if the Decisional Diffie-Hellman (DDH) problem is hard in G_2 then f_Q is strongly one-way.
(A Strong One-Way function is a function which is easy to compute and can be inverted only with a negligible probability on a random input or it is hard to invert on all but a negligible fraction of inputs.)

——-The End———