Cryptography (BITS F463) Comprehensive Exam (2022)

There are 5 questions in all and total marks are $5+(5+5)+10+10+10 = 45$. Please show all steps in proofs or computations (using efficient algorithms). Calculators are allowed. This is an **open book exam**. You can use books or notes (only hard copies). Time: 180 minutes.

1. Caesar wants to arrange a secret meeting with Marc Anthony, either at the Tiber (the river) or at the Coliseum (the arena). He sends the ciphertext

   `EVIRE.`

   However, Anthony does not know the key, so he tries all possibilities. Where will he meet Caesar?

2. Suppose E and F are two encryption methods. Let K_1 and K_2 be keys and consider the double encryption

   $$G_{K_1,K_2}(m) = E_{K_1}\left(F_{K_2}(m)\right).$$

   (a) Suppose you know a plaintext-ciphertext pair. Show how to perform a meet-in-the-middle attack on this double encryption.

   (b) An *Affine Encryption* given by $x \to \alpha x + \beta (\text{mod } 26)$ can be regarded as a double encryption, where one encryption is multiplying the plaintext by α and the other is a shift by β. Assume that you have a plaintext and ciphertext that are long enough that α and β are unique. Show that the meet-in-the-middle attack from part (a) takes at most 38 steps (not including the comparisons between the lists)

3. Consider the *ElGamal Digital Signature Scheme*. The public key is (y, p, g), where $y \equiv g^x (\text{mod } p)$, p is a prime, and g is a generator for $\mathbb{Z}_p^*$. The secret key is x such that $y \equiv g^x (\text{mod } p)$. The signature of message m is a pair (r, s) such that $0 \neq r, s \neq p-1$ and $g^m \equiv y^r r^s (\text{mod } p)$. We choose a random number k such that $0 \neq k \neq p-1$ and gcd(k, p - 1) $= 1$ and set $r = g^k (\text{mod } p)$.

   Alice wants to sign a document using the ElGamal signature scheme. Suppose her random number generator is broken, so she uses $k = x$ in the signature scheme. How will Eve notice this and how can Eve determine the values of k and x and thus break the system?

4. Allice and Bob are following the *Elliptic Curve Diffie-Hellman* protocol using the elliptic curve $y^2 \equiv x^3 + 9x + 17 (\text{mod } 23)$. The base point is $(16, 5)$, Alice's public key is $(12, 17)$, and Bob's public key is $(8, 7)$. Compute the shared secret between Alice and Bob.

5. Using Shamir's $(4, 8)$ secret sharing scheme with the parameter $p = 29$, we get

   $$D_1 = 14, D_3 = 15, D_6 = 25, D_4 = 8.$$

   Find the shared secret D, the remaining pieces D_2, D_4, D_5, D_7, and the polynomial $q(x)$.