06-20008 *Cryptography* The University of Birmingham
Autumn Semester 2019 School of Computer Science
David Galindo Week 9

Exercise Sheet 4 (Summative)

Solutions need to be handed in **before** ~~6 December~~ ~~9 December~~ 10 December, 5pm.

In this assignment, we study asymmetric cryptography based on the Discrete Logarithm problem. This is a **summative** assignment and hence counts towards your final module's mark.

1. Let $p = 23$.

   (a) Compute by hand and build the table: $\boxed{1}$

i	0	1	2	3	$\ldots 20$	21	22
$5^i \mod 23$	1						1

   (b) Compute by hand $\log_5 11$ and $\log_5 20$ in $\mathbb{Z}_{23}^\star$. $\boxed{1}$

2. Consider the following public key cipher with key generator algorithm KG and encryption algorithm Enc:

   Key generator KG: Alice generates a key as follows

   - Generate primes p, q such that q divides $p - 1$.
   - Let $g \in \mathbb{Z}_p^*$ be a generator of the subgroup $G_q \subseteq \mathbb{Z}_p^*$ with $\mathsf{ord}(G_q) = q$.
   - Choose random x, y from $\{0, \ldots, q - 1\}$.
   - Compute $h_1 = g^x \mod p$ and $h_2 = g^y \mod p$.
   - Publish the public key $PK = (p, q, g, h_1, h_2)$.
   - Retain the private key pair $SK = (x, y)$.

   Encryption algorithm Enc: To encrypt a message $M \in G_q$ to Alice using her public key $PK = (p, q, g, h_1, h_2)$, Bob computes the following steps

   - Choose random $z \in \{0, \ldots, q-1\}$, calculate $c_1 = g^z \mod p$ and $c_2 = M \cdot h_1^{-z} \cdot h_2^z \mod p$.
   - The ciphertext is then $C = (c_1, c_2)$.

   Note that all multiplications are modulo p.

   (a) Design an appropriate decryption algorithm Dec for the cipher and demonstrate its correctness (i.e. $\mathsf{Dec}(SK, \mathsf{Enc}(PK, M)) = M$ for $\mathsf{KG}() = (PK, SK)$). $\boxed{2}$

   (b) Assume that we run the encryption algorithm $\mathsf{Enc}(PK, \cdot)$ with the parameters $PK = (p = 23, q = 11, g = 6, h_1 = ?, h_2 = ?)$, $SK = (x = 9, y = 8)$. Use the decryption algorithm $\mathsf{Dec}(SK, C)$ in order to decrypt the ciphertext $C = (3, 10)$. $\boxed{1}$

3. Let consider the following variant of the El-Gamal encryption scheme.

   Key Generation KG: Let G_q be a subgroup of prime order q of $\mathbb{Z}_p^*$ for prime p and let g be a generator of G_q. Let $H : \{0,1\}^* \to \{0,1\}^n$ be a hash-function. Let x be a random integer between 0 and $q-1$. Let $y = g^x \mod p$. The public-key is (p, q, g, y, H) and the private-key is x.

   Encryption Enc: Given $m \in \{0,1\}^n$, generate a random integer r between 0 and $q-1$ and let :

$$c = (g^r, H(y^r) \oplus m)$$

   (a) Design an appropriate decryption algorithm Dec for the cipher and demonstrate its correctness (i.e. $\mathsf{Dec}(SK, \mathsf{Enc}(PK, M)) = M$ for $\mathsf{KG}() = (PK, SK)$). $\boxed{1}$

   (b) Describe a chosen-ciphertext attack (CCA attack) against this variant. $\boxed{2}$

Total points: 8