Cryptography HW 2

Deadline: 11/24

Problem 1 [20pt]. Let $H : M \to T$ be a random hash function where $|M| \gg |T|$. In the lecture we showed that finding a collision on H can be done with $O(|T|^{1/2})$ random samples of H. How many random samples would it take until we obtain a three way collision, namely distinct strings x, y, z in M such that $H(x) = H(y) = H(z)$? Justify your answer.

(a) $O(|T|^{2/3})$
(b) $O(|T|^{3/4})$
(c) $O(|T|)$
(d) $O(|T|^{1/4})$

Problem 2 [30pt]. Let (Gen, E, D) be a chosen ciphertext secure public-key encryption system with message space $\{0,1\}^{128}$. Which of the following is also chosen ciphertext secure? Justify your answer.

(a) (Gen, E_1, D_1) where $E_1(pk, m) = (E(pk, m), 0^{128})$ and $D_1(sk, (c_1, c_2)) = \begin{cases} D(sk, c_1) & \text{if } c_2 = 0^{128} \\ \perp & \text{otherwise} \end{cases}$

(b) (Gen, E_2, D_2) where $E_2(pk, m) = (c_1, c_2)$ for $c_1, c_2 \leftarrow E(pk, m)$ and $D_2(sk, (c_1, c_2)) = D(sk, c_1)$

(c) (Gen, E_3, D_3) where $E_3(pk, m) = (E(pk, m), E(pk, 0^{128}))$ and $D_3(sk, (c_1, c_2)) = \begin{cases} D(sk, c_1) & \text{if } D(sk, c_2) = 0^{128} \\ \perp & \text{otherwise} \end{cases}$

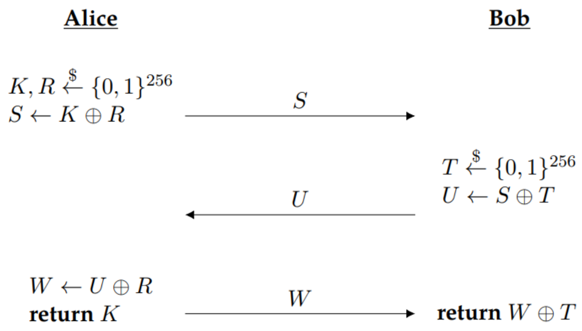
Problem 3 [20pt]. An administrator comes up with the following key management scheme: he generates an RSA modulus N and an element $s \in \mathbb{Z}_N^*$. He then gives user number i the secret key $s_i = s^{r_i}$ in $\mathbb{Z}_N$ where r_i is the i-th prime (i.e., 2 is the first prime, 3 is the second, and so on). Now, the administrator encrypts a file that is accessible to users i, j and t with the key $k = s^{r_i r_j r_t} \in \mathbb{Z}_N$. It is easy to see that each of the three users can compute k. For example, user i computes k as $k = (s_i)^{r_j r_t}$. The administrator hopes that other than users i, j and t, no other user can compute k and access the file. Unfortunately, this system is terribly insecure. Prove that any two colluding users can combine their secret keys to recover the master secret s and then access all files on the system.

Problem 4 [15pt]. Let G be a finite cyclic group of order n and consider the following textbook ElGamal encryption in G:

- $Gen()$: Choose a random generator g of G and a random $x \in \mathbb{Z}_n$. Output $pk = (g, h = g^x)$ and $sk = (g, x)$.
- $E(pk, m \in G)$: Choose a random $r \in \mathbb{Z}_n$ and output $(g^r, m \cdot h^r)$
- $D(sk, (c_0, c_1))$: Output c_1 / c_0^x

This variant can be shown to be semantically secure under an appropriate assumption about G. It is however not chosen-ciphertext secure because it is easy to compute on ciphertexts. Prove that it is easy to construct an encryption of $m_1 \cdot m_2$ when encryptions of m_1 and m_2 are given.

Problem 5 [15pt]. Consider the key-exchange protocol shown in the following figure. Show that Alice and Bob output the same key. Analyze the security of the scheme (i.e., either argue why an adversary can't obtain the shared key or show a concrete attack).



Alice
Bob
$K, R \xleftarrow{\$} \{0,1\}^{256}$
$S \leftarrow K \oplus R$
S
$T \xleftarrow{\$} \{0,1\}^{256}$
$U \leftarrow S \oplus T$
U
$W \leftarrow U \oplus R$
return K
W
return $W \oplus T$