CS 202 - Introduction to Applied Cryptography **Fall 2016**

Final

December 9, 2016 *Liangjian Chen*

Problem 1 **Solution:**

Π' is not a TDF, because multiple key would leak the information about the orignal message. for fix e, we will have following congruence modulo equations set.

$$\begin{aligned} c_1 &= m^e \mod n_1 \\ c_2 &= m^e \mod n_2 \\ c_3 &= m^e \mod n_3 \\ c_4 &= m^e \mod n_4 \\ &\dots \\ c_n &= m^e \mod n_n \end{aligned}$$

Denote N as $\prod_{i=1}^{n} n_i$.

By Chinese remainder theorem, we can easily calculate the $m^e \mod N$. Because N is very likely to be larger than m^e. If this case applied, m^e **over the integer**. Therefore the original message leaked.

This problem is same with the what was described in textbook in page 414 about attack plain RSA with sending the same message to multiple receivers.

Problem 2 **Solution:**

(a) No it is not CPA secure.
Intuitively, since not a random encryption, it is not a CPA secure. Formally, the adversary $\mathcal{A}$ simply request the encryption oracle to encrypt the message m_0 and m_1 to get c_0 and c_1. Then comparing them to the challenge message c to easily break the secure.

(b) No it is not CPA secure.
the output leak the r. Thus the adversary $\mathcal{A}$ could calculate the bitmask $F(pk, r)$ and recover the original message.

(c) Yes, it is CPA secure. Assume it is not CPA secure, and there is a PPT adversary $\mathcal{A}$ successfully attack $E(pk, m) = (F(pk, r), r \oplus m)$. Construct a new adversary $\mathcal{A}'$ against F as following:
get the $(F(pk, r), r \oplus m)$ from the encryption, and feed it to $\mathcal{A}$ to obtain m. Then easily get $r = r \oplus m \oplus m$ without the knowledge about td. Obviously, it is a PPT adversary, and with the non-eligible probability $Pr[\text{PubK}^{eav}_{\mathcal{A},\Pi} = 1]$, then $Pr[\text{Invert}_{A,f}(n) = 1] = Pr[\text{PubK}^{eav}_{\mathcal{A},\Pi} = 1]$ is still non-eligible. However it contrast with the assumption that F is a one-way function. Thus it is a CPA secure frame.

(d) Yes it is CPA secure. Compared to subproblem (c). m exclusive a random hash function of r. r is chosen randomly, and after encoding by a random hash function, it is still a random bit-string. So it is still a CPA-secure.

Problem 3 **Solution:**

Yes it is One-way function. Prove it by induction. First, if $B = 1$, $H^h_{1,IV}(x) = h(x)$, it must be one-way function.

Assume for any $B < b$, $H^h_{B,IV}(x)$ is one-way function. Consider the case when $B = b$.

First we can obtain that $H^h_{b,IV}(x) = h(H^h_{b-1,IV}(x_{[1:b-1]})||X_b)$. Since h is one-way, it is infeasible to get X_b and $H^h_{b-1,IV}(x_{[1:b-1]})$. Therefore it is infeasible to get $X_{[1:b]}$ (adversary even do not know the output of $H^h_{b-1,IV}$). Thus $H^h_{b,IV}(x)$ is a OWF. By induction, for all integer B, $H^h_{B,IV}(x)$ is OWF.

(X_i means i^{th} block in input. $X_{[1:n]}$ means first i blocks in input)

Problem 4 **Solution:**

Intuitively, since $G^{|m|}$ is a PRG, there is no way to recover the m except adversary has any information about r. However r is covered by a CPA-secure PKE which is computational infeasible to track. Thus this is a CPA-secure PKE.

Problem 5 **Solution:**

(a) It is KE secure against eavesdropper, but not successfully against man-in-the-middle(MITM).

Against eavesdropper:

From Diffie-Hellamn protocol(DHP), we know that it is impossible to obtain g^{ab} for Eve. Therefore it is impossible to obtain the $H(g^{ab})$ as well. Thus it is secure against eavesdropper.

Against MITM:

MIMT against DHP would result in that two parties use attacker's key. Therefore, even the key is hashed by H, as long as Mallory encode her key by H as well, it's still insecure.

(b) It is KE secure against eavesdropper, but not successfully against man-in-the-middle(MITM).

Against eavesdropper:

It is a CPA-secure public key encryption, so Eve is not able to recover or Bob's key. Thus, she can not send message to both side(failed in MAC). Also with out the private key she can not decrypt an message as well.

Against MITM:

First Mallory intercept Alice's public key, and send her public key to Bob. Then Mallory intercept Bob's MAC key, and send her MAC key to Alice. Though Mallory can not decrypt the message on Alice side and send message to Bob. However she can send message to Alice and decrypt the message from Bob. Thus it is still KE-insecure.

(c) It is KE secure against eavesdropper, but not successfully against man-in-the-middle(MITM).

Against eavesdropper:

This scheme is stronger than (b). (b) is enough against eavesdropper, therefore so as this scheme

Against MITM:

Same with(c). Because, by using public key encryption, Mallory lose her ability to decrypt Alice's message. Public key is supposed to be known by anyone. So hash the public key won't improve the secure. However, with the Bob's key, Mallory still can forge the message.

(d) It is KE secure against both eavesdropper and MITM.

Against eavesdropper:

It is same as the above one.

Against MIMT:

Now, Mallory only know the public key, she can not send message to both side because without MAC key she can not forge an message. Also without the private key, she can not decrypt the message as well. Thus it is KE secure.

Problem 6 **Solution:**

(a) assume a a signature(σ, y) on m. We can forge a new signature $(m-1, f(\sigma))$.

(b) the signature is a pair $(\sigma, \sigma') = (f^{n-m}(x), f^m(x'))$. And the verify procedure is check whether $y = f^m(\sigma),$ and $y' = f^{n-m}(\sigma')$.

Prove:

Assume, now we have a data with message m, signature (σ, σ'). For any other message m', either $m > m'$ or $n - m > n - m'$ must holds. Let's might as well assume it is $m > m'$. So to forge a new signature, we must know the preimage(or several order of preimage) of σ. However, f is an One-way, which infeasible to track preimage.

Thus, only way to obtain $f^{m'}(x')$ is random guessing. However the size of domain D is 2^n. So it is still infeasible.

Thus this signature is secure.