Principles of Information Security

Assignment- 2

1. (a) Explain Strong One way function and Weak One way function.
   (b) Prove "Weak one way functions exist if and only if strong one way functions exist".
   (c) Prove "A collection of one way functions exists if and only if one way functions exist".
2. Define the length-preserving, keyed function F by $F_k(x) = k \oplus x$. Prove that F is not a pseudo random function by describing and analyzing a concrete distinguisher.
3. Given a PRF F: $\{0,1\}^k$x$\{0,1\}^n \mapsto \{0,1\}^n$, construct a PRF G: $\{0,1\}^k$x$\{0,1\}^n \mapsto \{0,1\}^{2n}$, which is a secure PRF as long as F is secure.
4. Which of the following is collision resistant. Justify Your Answer
   (a) H'(m)=H(m)⊕H(m)
   (b) H'(m)=H(H(H(m)))
   (c) H'(m)=H(m)[0,...,31] (i.e. output the first 32 bits of the hash)
   (d) H'(m)=H($|m|$) (i.e. hash the length of m)
   (e) H'(m)=H(m)⊕H(m⊕$1^{|m|}$) (where m ⊕$1^{|m|}$ is the complement of m)
   (f) H'(m)=H(m)‖H(m)
   (g) H'(m)=H(H(m))

   Assuming H: $M \mapsto T$ be a collision resistant hash function. and ‖ represents the Concatenation
5. (a) What do you understand by Merkle-Demgard Transform? Explain its Construction Briefly.
   (b) Is it necessary that the Hash Function generated from Merkle-Demgard tranform will be Collision free if the initial Fixed length hash function was collision free? Prove your Answer.
6. Tell whether these are true or False and Justify your answer in brief (Either By explanation or by example):
   (a) Collision resistance implies 2nd-preimage resistance of hash functions.
   (b) collision resistance does not guarantee preimage resistance.
   (c) Let h_k be a keyed hash function which is a MAC algorithm (thus has the property of computation-resistance). Then h_k is, against chosen-text attack by an adversary without knowledge of the key k,

i. both 2nd-preimage resistant and collision resistant; and

ii. preimage resistant (with respect to the hash-input).

(d) If either h_1 or h_2 is a collision resistant hash function, then h(x) = h_1 (x) $\|$ h_2(x) is a collision resistant hash function.

7. *Note:* Read the Concept below before attempting the questions:
A Hash Family is Considered as a four Tuples (X,Y,K,H), where X a set (finite or Infinite) of Possible Messages , Y is the finite set of possible Message digests, K is the Key Space which is a finite set of possible Keys, for each k ϵ K, there exists a Hash Function $h_k \epsilon H$. A Pair (x,y) is valid pair if h_k(x)=y. Let $F^{X,Y}$ denotes the set of all hash functions. Suppose $|X| = N$, and $|Y| = M$. Then clearly, $\left|F^{X,Y}\right| = M^N$. Any hash Family F$\subseteq F^{X,Y}$ is known as (N,M) hash Family.
The Random Oracle Model Attempts to capture the concept of a ideal hash function. If a hash function h is well designed , it should be the case that the only efficient way to determine the value of h(x) for a given x is to evaluate the value x on the function x. This should not be the case that if $h(x_1), h(x_2)$ is already computed then there exists a x_3 such that $h(x_3)$ can be calculated from the previously computed hash values.
Theorem 1: suppose h $\epsilon F^{x,y}$ are chosen randomly and let $X_0 \subseteq X$. Suppose that the value h(x) have been determined (by querying for h) if and only if $x \epsilon X_0$. Then the Pr[h(x)=y] = 1/M for all $x \epsilon X - X_0$ and all yϵY.

From security Point of View, Some algorithms are discussed as below along wit there pseudo code:

Problem 1: PriImage
Instances: A hash Function h: $X \mapsto Y$
Find: x ϵ X such that h(x) = y.
Algorithms 1: Find-PreImage (h,y,Q)
choose any $X_0 \subset X$,$|X_0| = Q$

```
for each x in X_0:
    if (h(x)==y):
        return (x)
return (failure)
```

Problem 2: Second PreImage
Instances: A Hash function h: $X \mapsto Y$ and an element $x \epsilon X$.
Find: $x' \epsilon X$ such that x' != x and h(x')=h(x).
Algorithms 2: Find-Second-PreImage (h,x,Q)
y = h(x)
choose any $X_0 \subset X\{X_0$,$|X_0| = Q - 1$

```
for each x0 in  X_0$:
    if (h(x0)==y):
        return (x0)
return (failure)
```

Problem 3: Collision
Instances: A Hash function h: $X \mapsto Y$.
Find: $x, x' \epsilon X$ such that x' != x and h(x')=h(x).
Algorithm 3: Find-Collision (h,Q)
choose any $X_0 \subset X$,$|X_0| = Q$

```
for each x in X_0$:
      y_x = h(x)
if (y_x==y_x') for some x'!=x:
         return (x,x')
else return (failure)
```

Prove or refute:

(a) suppose that the hash function h: Z_nx$Z_n \mapsto Z_n$ is a linear function given by h(x,y)=ax+by mod n for a,b ϵZ_n and $n >= 2$ is a positive Integer. h follows the radical oracle model.

(b) For any $X_0 \subseteq X$ with $abs(X_0) = Q$, The Average case success probability of the algorithm 1 is p = 1-$(1 - 1/M)^Q$.

(c) For any $X_0 \subseteq X - \{x\}$ with $abs(X_0) = Q - 1$, The Average case success probability of the algorithm 2 is p = 1-$(1 - 1/M)^{Q-1}$.

(d) For any $X_0 \subseteq X$ with $abs(X_0) = Q$, The Average case success probability of the algorithm 3 is p = 1-[{(M-1)/M}*{(M-1)/M}*....{(M-Q+1)/M}]

8. if we define a hash function (or comparison function) h that will hash an n-bit binary string to an m-bit binary string, we can view h as a function from Z_{2^n} to Z_{2^m},it is tempting to define h using operation modulo 2^m. suppose that $n = m > 1$, and h:$Z_{2^m} \mapsto Z_{2^m}$ is defined as: h(x) = $x^2 + ax + b$ mod 2^m. Prove that it is easy to solve second primage for any x ϵZ_{2^m} without having to solve the quadratic equation.

9. Consider a hash function h which is second PreImage and Collision resistant and Defined as $h : \{0,1\}^* \mapsto \{0,1\}^n$. Consider Another hash function h_1 which is defined as follow: $h_1 : \{0,1\}^* \mapsto \{0,1\}^{n+1}$ and given by rule :

$h_1 = \begin{cases} 0\|x & \text{if } x\epsilon\{0,1\}^n \\ 1\|h(x) & \text{otherwise} \end{cases}$ Prove that h_1 is not preimage resistant but still second preimage and collision resistant.

10. suppose h_1: $\{0,1\}^{2m} \mapsto \{0,1\}^m$ is a collision resistent function.

(a) Define h_2: $\{0,1\}^{4m} \mapsto \{0,1\}^m$ as follow:
   i. write x ϵ $\{0,1\}^{4m}$ as x= $x_1 \parallel x_2$ where $x_1, x_2 \epsilon \{0,1\}^{2m}$.
   ii. Define $h_2(x) = h_1(h_1(x_1)\|h_1(x_2))$.

Prove that h_2 is collision resistant.

(b) for any integer $i >= 2$, Define has function h_i: $\{0,1\}^{2^i m} \mapsto \{0,1\}^m$ recursively from h_{i-1} as follow:

   i. write $x \epsilon \{0,1\}^{2^i m}$ as $x = x_1 \parallel x_2$ where $x_1, x_2 \epsilon \{0,1\}^{2^{i-1} m}$.

   ii. Define $h_i(x) = h_{i-1}(h_{i-1}(x_1) \| h_{i-1}(x_2))$.

Prove that h_i is collision resistant.

11. Let m be a message consisting of l AES blocks (say l=100). Alice encrypts m using CBC mode and transmits the resulting ciphertext to Bob. Due to a network error, ciphertext block number $l/2$ is corrupted during transmission. All other ciphertext blocks are transmitted and received correctly. Once Bob decrypts the received ciphertext, how many plaintext blocks will be corrupted?