CS:6160 CRYPTOLOGY

PRACTICE QUESTIONS

Instructions

- Try these questions before class. Do not submit!
- We will discuss the solutions on September 2, 2022

(1) Assume an attacker knows that a user's password is either *abcd* or *bedg*. Say the user encrypts his password using the shift cipher, and the attacker sees the resulting ciphertext. Show how the attacker can determine the user's password, or explain why this is not possible.

(2) Provide a formal definition of the *Gen*, *Enc*, and *Dec* algorithms for the shift cipher.

(3) Provide a formal definition of the *Gen*, *Enc*, and *Dec* algorithms for the Vigenère cipher.

(4) Say we have a scheme with a claimed proof of security with respect to some definition, based on some assumption. The scheme was successfully attacked when used in the real world. What are possible reasons for this?

(5) If $f(n)$ and $g(n)$ are two negligible functions, then their sum $h(n) = f(n)+g(n)$ is also negligible.

(6) Consider an encryption scheme (Gen, Enc, Dec) where for any two messages $m, m^{'} \in \mathcal{M}$ the distribution of the ciphertext when m is encrypted is identical to the distribution of the ciphertext when $m^{'}$ is encrypted. i.e.

$$Pr[Enc_K(m) = c] = Pr[Enc_K(m^{'}) = c], \forall c \in \mathcal{C}$$

Q: Show that the above definition is equivalent to saying that an encryption scheme is perfectly secret.

(7) We give below the definition of perfect (adversarial) indistinguishability which is slightly different from the above definition but also gives another equivalent definition of perfect secrecy. This definition is based on an experiment involving an adversary passively observing a ciphertext and then trying to guess

which two possible messages are encrypted. These kind of experiments are very common in proving security in cryptography.

Experiment :

(a) An adversary $\mathcal{A}$ first specifies two arbitrary messages $m_0, m_1 \in \mathcal{M}$.

(b) A bit $b \in \{0,1\}$ is randomly chosen and m_b is encrypted. These actions are hidden from the adversary.

(c) The resulting ciphertext is given to $\mathcal{A}$.

(d) $\mathcal{A}$ outputs a guess as to which one of the two messages was encrypted.

(e) $\mathcal{A}$ succeeds this experiment if it guesses correctly.

An encryption scheme is said to *perfectly indistinguishable* if no adversary $\mathcal{A}$ can succeed with probability better than 1/2. Note that $\mathcal{A}$ can succeed with probability 1/2 by outputting a uniform guess, so the requirement is that an attacker does better than that.

Q: Show that the notion of perfectly indistinguishable is equivalent to perfect secrecy.

(8) Is the One Time Pad secure against chosen ciphertext attack?

(9) You have a randomly chosen key k of length n and a message m of length $n-2$ to be encrypted. You come up with the following encryption scheme:

$$Enc_k(m) = k \oplus (01 \circ m), m \in \{0,1\}^{n-2}, k \in \{0,1\}^n,$$

where $\circ$ is the concatenation operator. That is, 01 is appended to m in the beginning to get a string of length n. Does this scheme provide perfect secrecy?

(10) You have a mechanism to generate random keys of length k and l s.t. $k+l = n-1$. The message you want to encrypt is of length n. To encrypt this message you come with the following scheme:

$$Enc_{k_1,k_2}(m) = (k_1 \circ 1 \circ k_2) \oplus m, m \in \{0,1\}^n, k_1 \in \{0,1\}^k, k_2 \in \{0,1\}^l.$$

Does this scheme provide perfect secrecy?

(11) Show that

$$\mathbb{Z}_n{}^* = \{x : x \in \mathbb{Z}_n \text{ and } \gcd(x,n) = 1\}$$

is a multiplicative group.

(12) Show that there exist an inverse d for $e \mod m$, $ed \equiv 1 \mod m$ iff $\gcd(e,m) = 1$.

(13) For prime p, $\mathbb{Z}_p{}^*$ has at least ONE element g with order $p-1$. $\{g^1, g^2, \ldots, g^{p-1}\} = \mathbb{Z}_p{}^*$.

(14) Define order of an element in a group. Show that the order of an element divides the order of a group for a finite group. What is the order of a generator of a finite cyclic group?

(15) Which of the following are one-way functions? For each function that is a one-way function, explain why (no formal proof required). For each function that is not a one-way function, describe a polynomial-time attack (i.e., describe how, given y, one can find a preimage x in polynomial-time with non-negligible probability). Remember that to break a one-way function, it is sufficient to find some preimage, not necessarily the original input to the one-way function.

(a) $f_1(x) = 0$ for all $x \in \{0, 1\}^n$, for a finite size domain.

(b) $f_1(x) = x_1 \dots x_{n/2}$ for all $x \in \{0, 1\}^n$.

(c) $f(x) = g(x)||g(x)$, where g is any OWF.

(16) Show that the RSA OWF discussed in class is a permutation. *Hint: It is enough to show that it is one-one. Since its a finite set, if it is a one-one function it implies its surjective too! Show!*

August 23, 2022 ; Dept of CSE, IIT Hyderabad