Vrudresh.

18733: Applied Cryptography S17
HomeWork 1.

Distribution of a PRF [3 points]

Given: $F: \{0,1\}^k \times \{0,1\}^l \rightarrow \{0,1\}^L$ is a secure PRF

$$x \in \{0,1\}^l \; ; \; y \in \{0,1\}^L$$

To prove: $\frac{1}{2^L} - \varepsilon \leq Pr[F(k,x) = y : k \leftarrow_R \{0,1\}^k] \leq \frac{1}{2^L} + \varepsilon$

Assumption: F is not a uniform distribution and not secure.

Proof: 1) The high probability of occurrence of cipher text c_1 from message m_1 and using key k is.

$$Pr[F(k, m_1) = c_1] \geq \frac{1}{2^L} + \varepsilon$$

2) The lower probability of occurrence of cipher text c_1 from message m_1 and using key k is:

$$Pr[F(k, m_1) = c_1] \leq \frac{1}{2^L} - \varepsilon$$

From 1 and 2 and ε being is non-negligible value.

$$\left(\frac{1}{2^L} + \varepsilon\right) \leq Pr[F(k, m_1) = c_1] \leq \left(\frac{1}{2^L} - \varepsilon\right)$$; which states that an adversary A has an advantage of ε if F is a secure PRG,

i.e $Pr[A(r) = 1] = \frac{1}{2^L}$ — 3

$Pr[(A(F(k)) = 1] \leq \frac{1}{2^L} + \varepsilon$ — 4

$$Adv_{PRG}(A, F) = |\, 4 - 3 \,| \leq \varepsilon$$

Therefore, if F is not secure, the adversary A's advantage would not be negligible. Also, a secure PRF is indistinguishable from Random F (3). Therefore, a secure PRF is also uniformly distributed

Secure Blockciphers [4 points]

Given: Block cipher $E : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a secure PRP.

a) To prove: $E'_K(x \| x') = E_K(x) \| E_K(x \oplus x')$ is not secure;

i.e. a random ~~function~~ permutation in E' is distinguishable from a random ~~function~~ permutation in S_F (in a subset of E'_K.)

Proof:

$$E_K(x) \rightarrow \{0,1\}^n. \quad (1)$$

$$E_K(x \oplus x') \rightarrow \{0,1\}^n. \quad (2)$$

$$E_K(x) \| E_K(x \oplus x') \rightarrow \{0,1\}^n. \quad (3).$$

x	x'	$x \oplus x'$
0	0	1
0	1	0
1	0	0
1	1	1

(1) is a secure PRP, (2) is not secure as the a random permutation chosen from (2) would be distinguishable from E_K (2) as shown in the table alongside. i.e

$$Adv[(random\ (2)) - (2)] > \varepsilon$$

Since, (2) is in distinguishable and (3) has a portion of it which is distinguishable, (3) as a whole becomes distinguishable from a randomly chosen permutation of (3).

Therefore, $E'_K(x \| x')$ is not secure

Scanned by CamScanner

Secure Blockciphers [4 points]

b) $E^{(2)} : \{0,1\}^{2k} \times \{0,1\}^{n} \longrightarrow \{0,1\}^{n}$ defined by.

$G \qquad K \qquad X \qquad X$

$$E^{(2)}_{K_1 \| K_1}(x) = E_{K_1}(E_{K_2}(x)).$$

$$K_1, K_2 \in \{0,1\}^{k} \;\&\; x \in \{0,1\}^{n}.$$

To prove: $E^{(2)}$ is secure PRP.

Given: $E : \{0,1\}^{k} \times \{0,1\}^{n} \rightarrow \{0,1\}^{n}$ is a secure PRP.

$K \quad X \quad X \longrightarrow X$

i.e. $\begin{cases} \text{Perms}[x] : \text{the set of all } \underline{\text{one-to-on}} \text{ function } X \text{ to } X. \\ S_F = \{ E(k, \cdot) \text{ such that } k \in K \} \subseteq \text{Perm}[X] \end{cases}$

Proof: A PRP is secure if a random function in Perm[X] is indistinguishable from a random function in S_F

In our case, $E : \{0,1\}^{k} \times \{0,1\}^{n} \rightarrow \{0,1\}^{n}$ is given as secure and

$E^{(2)}$ being an extension of E, it can be said that, $G : K \longrightarrow \{0,1\}^{nt}$ is a secure PRG.

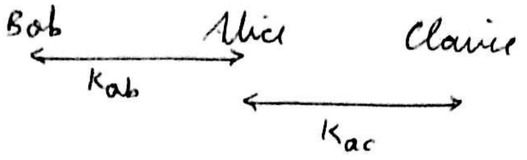
i.e; $E^{(2)} : \{0,1\}^{2k}$ is a secure PRG. and a secure PRF,

but, the given $E^{(2)}$ is a deterministic algorithm. and a one-to-one function and from the extension of E, it can be said that, there also exits an "efficient" inversion algorithm and. provided that $E^{(2)}$ is indistinguishable from random function $E'^{(2)}$ from the key PRF property being encapsulation - Given $E^{(2)}$ is therefore a secure PRP.

Secret Sharing with Block Ciphers [4].

Given: Block cipher $E(k, m)$ be secure.

a)



$|d| = p + l$ for some $l \geq 1$

① — Let Alice use key k to encrypt message $m \Rightarrow k(m)$

② — Let Alice encrypt a ~~message~~ key ~~k~~ using K_{ab} and K_{ac}. $\Rightarrow K_{ab}(K_{ac}(\cancel{k}))$

③ — Finally, Alice can ~~send~~ concatenate ② ~~to~~ and ①.

$\Rightarrow K_{ab}(K_{ac}(\cancel{k})) \,||\, k(m)$

$\therefore$ Bob can decrypt ③ using key K_{ab} to obtain k.
Clarice can decrypt ③ using key K_{ac} to obtain k.
On obtaining key k, Bob and Clarice can use k to decrypt the message m.

b) Alice encrypts the message m with key k.
Alice encrypts the key k with either $K_{ab}K_{ac}$, $K_{ab}K_{ad}$ or $K_{ac}K_{ad}$ as follows:

~~$E_{(K_{ab})}[E(K_{ac}(k))] \,||\, E_{(K_{AC})}[E(K_{ad})$~~

$$E_{K_{ab}}[E_{K_{ac}}(k)] \,||\, E_{(K_{AC})}[E_{K_{ad}}(k)] \,||\, E_{K_{ab}}[E_{K_{ad}}(k)] \,||\, E_k(m)$$

Any two can then co-operatively obtain the message.

c) As number of recipients increases, size of solution increases.
Therefore $^nC_t = \dfrac{n!}{t!\,(n-t)!}$ = size of cipher text, i.e. t can encrypt

$$^nC_{t-1} = \frac{n!}{(t-1)!\,(n-t+1)!} \Rightarrow t-1 \text{ cannot encrypt}$$

$\therefore$ Size of the cipher text $= {}^nC_t + |E(k, m)|$

$$= \frac{n!}{t!\,(n-t)!} + |E(k, m)|$$

Scanned by CamScanner

Identity (Key) - Hiding Encryption [4 points].

a) Example of IND-CPA secure encryption scheme that has this identity (key) revealing.

⇒ Consider an IND-CPA ~~set~~ scheme that has encrypt (E_S) and Decrypt (D_S). Consider another scheme with Encrypt (E) and decrypt (D). Let us assume that both keys produce the same key K.

Let E run $E_S(K, x)$ to get ciphertext C, and return $C || H(K)$ where $H(x)$ is a collision resistant one way hash function. Let D simply discard the hash part of the cipher text and use D_S to decrypt.

If, E_S & D_S form an IND-CPA secure encryption schem, E & D also form an IND-CPA secure schem, but ~~the~~ it is indentity revealing.

b). Let there be a central authority that generates a master public key K and private key K_P.

- The challenger can use its ID and the public K to generate its own public key K_{CP}
- The challenger can obtain ~~th~~ its private key by contacting the central authority to obtain K_P ~~along~~ and combing it with its available ID.
- When adversary provides the plaintexts m_0 and m_1 to the challenger, the cipher text so obtained remain indistinguishable and the ID used for encryption is not revealed either.
- The adversary is said to have negligible "advantage" ε, if it wins the above game with the probability $\frac{1}{2} + \varepsilon(k)$, although the adversary knows m_0 & m_1, the probabilistic nature of E means that the encryption M_b will be only one of many valid ciphertexts, and ∴ $E(m_0, m_1)$ & comparison with C_0, C_1 does not afford any negligible advantage to the adversary.

Scanned by CamScanner

Stream Cipher Re-use [5 points]

1) — Program attached and screenshot of the output provided as well.

2). Yes, the attack would be possible. The trick to decoding/decrypting the message was ~~to~~ ~~assume~~ based on the assumption that a particular "letter" would be encoded/encrypted similarly across all plaintext. Therefore, by comparison, of the plaintext (whether random or not) can be obtained in its initial form.

3) No, the attack would not be possible as the number of sample space is limited (3 for example). One would not be able to decode all the letters with certainity.

For example:

If encoded message m_1 is: abcde

m_2 is: fghijk

m_3 is lmnop.

From the above samples we can see that there is no commonality in the encoded texts to be able to decipher the plaintext accuratitly.

Chosen Ciphertext Attack [5 point]

a) Definition of security game.

Challenger | **Adversary**

1) generate PK, SK based on k. $\xrightarrow{\text{sends PK.}}$ 1) perform encryption with PK and

$\longleftarrow$ sends to challenger C_0, C_1

2) sends ciphertext $C = E(SK, M_b)$ to adversary. $\xleftarrow{m_0 \; m_1}$ sends plaintext m_0, m_1.

$\longrightarrow$

$\longleftarrow$ outputs b.

Adversary advantage has to be negligible for winning the above game.

It is to be noted that the adversary can make any number of encryption and request for decryption to the oracle to determine the plaintext or the key.

b). Prove using reduction that IND-CCA security implies IND-CPA security.

⇒ IND-CPA security implies that the ciphertext so obtained from the plaintext m_0 and m_1 is indistinguishable. Similarly, it is to be proven that the IND-CCA security is such that the plain ~~cipher~~ text so revealed to the adversary are indistinguishable. and the advantage of the attacker is negligible.

From the attacker's output b', when $b = \{0,1\}^n$

– We define the advantage of a attacker A in the IND-CCA security game to be.

corresponds to message m_0 & m_1

$$Adv_A = Pr[b' = b] - 1/2 \;;$$

$$Adv_A = negligible\,(n)$$

≈ 0 → which is IND-CPA secure

Chosen Ciphertext Attack [5]

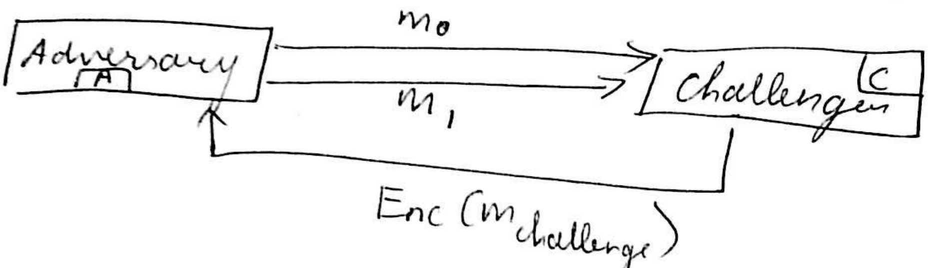
c). IND-CCA is basically the maximum amount of power one can give to the adversary without revealing the secret key.

Therefore IND-CCA does imply identity-hiding security.

Proof:

- Adversary chooses many messages and many ciphertexts, receives corresponding message-ciphertext pairs

$m_{challenge} = m_0, m_1$



$$Adv_A\left[Pr(Enc(m_0)) - Pr(Enc(m_1)) \right] = \varepsilon ;$$

i.e, cannot guess the encrypted message with more than negligible advantage (ε).

Note that this is similar to the "lunchtime attack", where the adversary sneaks into the office during lunch hour and has full access to the decryption circuit, but the key is kept secure in a hardware component.

Scanned by CamScanner