18733: Applied Cryptography S17

Homework 1

due February 10, 2017, 11:30am EST

Distribution of a PRF [3 points]

Let $F : \{0,1\}^k \times \{0,1\}^l \to \{0,1\}^L$ be a secure finite PRF. Fix $x \in \{0,1\}^l, y \in \{0,1\}^L$. Use a reduction proof to show the probability of any image of the function is close to uniform when taken over the randomness of the key k, i.e.,

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

Hint: Try showing this using contraposition.

Secure Blockciphers [4 points]

Let a block cipher $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a secure PRP.

(a) **[2 points]** Consider the family of permutations $E' : \{0,1\}^k \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ defined for all $x, x' \in \{0,1\}^n$ as

$$E'_K(x||x') = E_K(x)||E_K(x \oplus x').$$

Show that E' is not a secure PRP.

(b) **[2 points]** The *two-fold cascade* of E is the block cipher $E^{(2)} : \{0,1\}^{2k} \times \{0,1\}^n \to \{0,1\}^n$ defined by

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

for all $K_1, K_2 \in \{0,1\}^k$ and all $x \in \{0,1\}^n$. Prove that $E^{(2)}$ is a secure PRP.

Secret Sharing with Block Ciphers [4 points]

Let a block cipher $E(k,m)$ be secure.

(a) **[1 point]** Let Alice and Bob share a block cipher key K_{ab} while Alice and Charlie share a block cipher key K_{ac}. Using block cipher $E(k,m)$, define an encryption scheme that allows Alice to encrypt p-block message in such a way that it can only be decrypted cooperatively by both Bob and Charlie. The resulting ciphertext should be a constant number of blocks longer than the plaintext, i.e. $|c| = p + l$ for some $l \geq 1$.

(b) **[2 points]** In addition to K_{ab} and K_{ac} shared with Bob and Charlie, Alice shares a key K_{ad} with David. Using block cipher $E(k,m)$, define an encryption scheme for Alice to encrypt p-block message such that it can only be decrypted by any two cooperating people (ex. Bob and David). The resulting ciphertext should be a constant number of blocks longer than the plaintext, i.e. $|c| = p + l$ for some $l \geq 1$.

(c) **[1 point]** How does the size of your solution for (b) scale with the number of recipients? If there are n recipients and the encryption scheme allows any t out of n can decrypt but $t-1$ cannot, what would be the size of the ciphertext as a function of n and t? You don't have to prove the result.

Identity(Key)-Hiding Encryption [4 points]

An IND-CPA secure encryption scheme might not conceal identities, in the following sense: given a pair of ciphertexts C, C for equal-length messages, it might be "obvious" if the ciphertexts were encrypted using the same random key or were encrypted using two different random keys.

(a) **[2 points]** Give an example of a (plausibly) IND-CPA secure encryption scheme that has this identity(key) revealing.

(b) **[2 points]** Give a definition for "identity(key)-hiding" encryption by designing a security game. Your security definition should imply IND-CPA security but a scheme meeting your definition cant be identity(key)-revealing.

Hint: Get hints from the IND-CPA security game – how does the security game defined? What is the adversary's ability? How is the advantage of the adversary expressed? What is Exp0 and what is Exp1? Define the security game in these terms.

(Programming) Stream Cipher Re-use [5 points]

In this problem you are going to explore the consequences of when a stream cipher is used incorrectly. Suppose that a stream cipher key (which is supposed to be used ephemerally) is used more than once. Let us assume that a person W is using a single stream cipher key to send 10 messages to the other person H. The messages contain only the characters in the set $[a-z]$. Below are hex encoded 10 encrypted messages. The encrypted response from H, is also encrypted with the same stream cipher key, and the plaintext only contains characters in $[A-Z] \cup [a-z] \cup \{space\} \cup \{.\} \cup \{,\}$. Figure 1 shows 10 encrypted messages and the response respectively. Also, Figure 2 contains part of the code used to generate ciphertexts.

Encrypted messages:

- 4a2c3819d63a04baa08757d3daa67deb114f30e8c199c8c6aae8fa2c5d9eea9a
- 533f280fc62512a4a98244cbdabc75e2184039f0d197c4d5b1f2e53b5394e196
- 5e2d3a04db3113a5a7924ecbd3a763f3125e34e5d59ddbdcbae0ef23469bf389
- 50222517cd2b18b1a59445dbceb877e10f5638e4d797ddd8a7e3e73e5483e290
- 473a2e16c53815bdb09c49d5c8a879e7025821eddb8cdbc9b3fae8394a92f482
- 5d362117de2203a9b99a5ec5d6ac7ae90a4425f9c685c5cea9efef285287f895
- 5b34371edf3d1fb7ba9558cadebe74f117532bf1cd9cceccaeebf3355a8be780
- 52333e0aca2f1fb6b48d40dec6b769f81f4c2efec293d6d0a2e5ff275291e38f
- 4f242f03d3280aacad9056c3dcb06de91a4d30e3cf89d0dfbcfcf62d429cec85
- 502c341cd73a08b9a18055ddd7ba70e41a4738f9cc95cad5b9e2f2255181e98d

Encrypted Response

- 7a392803d92704bdb18e0392d2a63be41e5432a9f49ec8cda4e4b3

Figure 1: Encrypted messages and response

1. **[3 points]** Write a program that takes as input the 11 ciphertexts and outputs the plaintext of the secret message. Submit the code and the output of your program.

```
import sys

def strxor(a, b): # XOR Strings a and b
    if len(a) > len(b):
        return "".join([chr(ord(x) ^ ord(y)) for (x, y) in zip(a[:len(b)], b)])
    else:
        return "".join([chr(ord(x) ^ ord(y)) for (x, y) in zip(a, b[:len(a)])])

def encrypt(key, msg):
    c = strxor(key, msg)
    return c

def main():
    key = urandom(1024)
    p_messages = [<SOME-SECRET-MSGS>]
    p_response = <A-SECRET-RESPONSE>
    c_messages = [encrypt(key, msg) for msg in p_messages]
    c_response = encrypt(key, p_response)
```

Figure 2: A `python` code used to generate encrypted messages

2. [**1 point**] Would this attack be possible if the plaintext for all 11 messages was random? Explain.
3. [**1 point**] Would this attack be possible if there were far fewer messages, 3 for example? Explain.

(Optional) Chosen Ciphertext Attack [5 points]

Adversary in IND-CPA security has ability to pick an arbitrary plaintexts and obtain encryption of the messages. Now let us add one more ability to the adversary that he can decrypt any ciphertext of his choice, other than the 'challenged' cihpertexts. Here, 'challenged' ciphertexts mean the ciphertext that he has to guess which 'experiment' it was from (left-or-right, real-or-random). Given these abilities, the adversary's goal is to guess whether the 'challenged' ciphertexts are the results of encrypting left or right plaintexts. We denote this adversary as a chosen ciphertext attack(CCA) adversary.

(a) [**1 point**] Define the notion of the semantic(IND) security over chosen ciphertext attack(CCA) adversary by defining a security game.

(b) [**2 points**] Prove using reduction that IND-CCA security implies IND-CPA security.

(c) [**2 points**] Recall from problem 4 that we defined the notion of identity(key)-hiding security. Does IND-CCA security imply identity-hiding security? That is, does an encryption scheme that is secure against chosen ciphertext attack adversary also secure against identity-revealing adversary? If your answer is yes, please give a brief sketch of proof. If no, please give a simple counterexample.