| CS4236 Quiz | Semester 2 AY13/14 | October 2, 2014 |
|---|---|---|
| Name: | | Student Id: |

[2 marks] **Question 1**

Consider the modes of operation on block ciphers. In some modes, the encryption (or decryption) of the whole message can be parallelized, so that the time taken to encrypt (or decrypt) a long message is about the same as the time taken to encrypt (or decrypt) a one-block message. Which of the following can be parallelized (answer Yes or No):

| | |
|---|---|
| (a) CTR mode encryption: | Yes |
| (b) CTR mode decryption: | Yes |
| (c) CBC mode encryption: | No |
| (d) CBC mode decryption: | Yes, given all IVs stored from enc |

[2 marks] **Question 2**

Consider a form of chosen plaintext attack on block cipher under ECB mode (hence there is no IV), where the block size is 128 bits. The adversary's goal is to determine a 128-bits plaintext $m=b_{128}b_{127}\ldots b_2b_1$. The adversary has access to an oracle that on input x, outputs the ciphertext of $m_x$ where $m_x$ denotes the 128-bits block containing the $x$ least significant bits of $m$, padded in front by zeros, i.e.

$$m_x = 00..00\ b_x \ldots b_2b_1.$$

For example, $m_0$=00…0, $m_1$=00… $b_1$, and $m_{128} = m$. Note that the oracle always uses the same encryption key. Your goal is to give a successful attack by filling in the missing pseudo-code below. (Do not write outside the box).

```
c= Oracle (0);  //Oracle(x) returns the ciphertext of m_x
for i=1 to 128 do
```

```
mx = Oracle(i);
Store mx into hashmap Store
```

```
end-for-loop;
Output b128b127b126...b2b1;
```

**Question 3**. Alice employs the encryption algorithm of one-time-pad to encrypt a 3-bit message. Alice has access to a truly random source that generates 2 independent bits, $r_1$ and $r_2$. Based on that, she generates the 3-bit key $k_1k_2k_3$ using the formula:

$k_1 = r_1$ .xor. $r_2$
$k_2 = 1$ .xor. $r_1$
$k_3 = r_2$

Pr[k1 = 0] = Pr[r1 xor r2 = 0] = Pr[r1 = 0 ^ r2 = 0] + Pr[r1 = 1 ^ r2 = 1] = 0.5
Bias of k1 = 0.5 -0.5 = 0

Pr[k2 = 0] = Pr[1 xor r1 =0] = Pr[r1 = 1] = 0.5
Bias of k2 = 0

[1 mark] What is the bias of $k_1$, $k_2$ and $k_3$?

Bias of k3 = 0

| | $k_1$ | $k_2$ | $k_3$ |
|---|---|---|---|
| bias | 0 | 0 | 0 |

[1 mark] Give a linear combination of $k_1$, $k_2$ and $k_3$ that has bias 0.5. Pr[k1 xor k2 xor k3 = 0] = 1

| |
|---|
| k1 = 0, k2 = 0, k3 = 0 |

[1 mark] What is the distribution of the 8 possible keys?

| K | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
|---|---|---|---|---|---|---|---|---|
| Probability | | | | | | | | |

1/8 for everything

[2 marks] Does Alice's method achieve perfect secrecy? Why?

Yes. Uniform distribution of key k = k1k2k3 => k xor 3-bit m from M leads to uniform distribution of c in C
We aim to prove Pr[M = m | C = c] = Pr[M = m]
By Bayes Thm,
Pr[M = m | C = c] = {Pr[C = c | M = m] x Pr[M = m]} / Pr[C =c]

Pr[C = c | M = m] = Pr[K = m xor c] = 1/8
Pr[C = c] = Pr[c = K xor m] = Pr[K = c xor m] = 1/8
Hence
Pr[M = m | C = c] = 1/8 * Pr[M = m] / 1/8 = Pr[M = m]

Suppose the plaintext follows this distribution:

| X | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
|---|---|---|---|---|---|---|---|---|
| Probability | 0 | 0.5 | 0.1 | 0.1 | 0.1 | 0 | 0.2 | 0 |

[1 mark] What is the probability that the ciphertext is 000?

**Pr[C = 000]**
**= Pr[000 = K xor m]**
**= Pr[K = 111, m =111] + Pr[K = 110, m = 110] + … + Pr[K = 000, m = 000]**
**= Pr[K=001, m=001] + Pr[K=010, m=010] + … (only those with m > 0)**
**= 1/8(0.5 + 0.1 + 0.1 + 0.1 + 0.2)**
**= 1/8 ?**

[1 mark] You are the eavesdropper and you are aware of Alice's algorithm and the distribution of the plaintext. You know that the ciphertext is 000. What is the conditional probability of the plaintext, given that the ciphertext is 000?

| X | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
|---|---|---|---|---|---|---|---|---|
| Probability | | | | | | | | |

[2 marks] You are the eavesdropper and you are aware of Alice's algorithm and the distribution of the plaintext. You know that the first two bits of the ciphertext is 00, but do not know the last bit of the ciphertext. So the ciphertext could be 000, or 001.

What is the probability that the ciphertext is 001?

What is the conditional probability of the plaintext, given that the first two bits of the ciphertext is 00?

| X | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
|---|---|---|---|---|---|---|---|---|
| Probability | | | | | | | | |

[2 marks] (Ciphertext Stealing) **Question 4**

In all modes of operations given in the lecture, the size of the ciphertext is always a multiple of the block size. Consider an application where the plaintext consists of (128+64=192) bits. An important requirement of the application is that, the ciphertext must be 192 bits. Suppose that the application wants to use a block cipher of 128 bits.

Your task here is to give an algorithm that on input the 192-bit plaintext, outputs a 192-bit ciphertext, using 2 calls to the block cipher encryption.

There is a technique known as "ciphertext stealing" that solves this problem. It is quite intuitive.

Let us define:

| | |
|---|---|
| E(x) | : Encrypt the 128-bit x using the block cipher. |
| \|\| | : Concatenation. |
| Head(x,m) | : The first m bits of x. |
| Tail(x,m) | : The last m bits of x. |

Fill in the missing few steps that on input a 192-bit plaintext x, generates C, the 192-bit ciphertext of x. It is important that there is a way to decrypt it.

Let $x_1$ = Head(x,128);
Let $x_3$ = Tail(x, 64);
$c_1$ = E( $x_1$ );
Let h = Head( $c_1$, 64);
Let t = Tail( $c_1$, 64);

Output C