Homework 2[1]

Question 1

Consider the following five events. What is the order of these events from most likely to least likely?

1. Correctly guessing a random 128-bit AES key on the first try.

2. Winning a lottery with 1 million contestants (the probability is $1/10^6$).

3. Winning a lottery with 1 million contestants 5 times in a row (the probability is $(1/10^6)^5$).

4. Winning a lottery with 1 million contestants 6 times in a row.

5. Winning a lottery with 1 million contestants 7 times in a row.

Question 2

Suppose that using commodity hardware it is possible to build a computer for about $200 that can brute force about 1 billion AES keys per second. Suppose an organization wants to run an exhaustive search for a single 128-bit AES key and was willing to spend 4 trillion dollars ($\$4 * 10^{12}$) to buy these machines (this is more than the annual US federal budget). How long would it take the organization to brute force this single 128-bit AES key with these machines? Ignore additional costs such as power and maintenance.

1. More than a million years but less than a billion (10^9) years.

2. More than a month but less than a year.

3. More than a 100 years but less than a million years.

4. More than a day but less than a week.

5. More than a billion (10^9) years.

Question 3

Let $F : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a secure PRF (i.e. a PRF where the key space, input space, and output space are all $\{0,1\}^n$ and say $n = 128$. Which of the following is a secure PRF (there is more than one correct answer):

1. $F'(k,\ x) = k \bigoplus x$

[1] `https://class.coursera.org/crypto-012/`

2. $F'(k, x) = \text{reverse}(F(k, x))$ where $\text{reverse}(y)$ reverses the string y so that the first bit of y is the last bit of $\text{reverse}(y)$, the second bit of y is the second to last bit of $\text{reverse}(y)$, and so on.

3. $F'(k, x) = F(k,\ x) \bigoplus F(k,\ x \oplus 1^n)$.

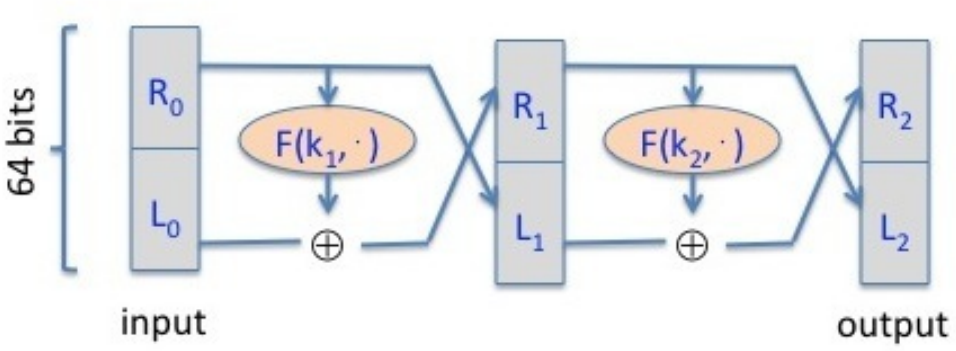
4. $F'(k, x) = F(k, x) \ \| \ 0$ (here $\|$ denotes concatenation)

5. $F'((k_1, k_2),\ x) = F(k_1, x) \ \| \ F(k_2, x)$ (here $\|$ denotes concatenation)

6. $F'(k, x) = F(k, x)[0, \ldots, n-2]$ (i.e., $F(k, x)$ drops the last bit of $F(k, x)$)

Question 4

Recall that the Luby-Rackoff theorem discussed in Lecture 3.2 states that applying a three round Feistel network to a secure PRF gives a secure block cipher. Let's see what goes wrong if we only use a two round Feistel. Let $F : K \times \{0,1\}^{32} \to \{0,1\}^{32}$ be a secure PRF. Recall that a 2-round Feistel defines the following PRP $F_2 : K^2 \times \{0,1\}^{64} \to \{0,1\}^{64}$. Here R_0 is the right 32 bits of the 64-bit input and L_0 is the left 32 bits.



One of the following lines is the output of this PRP F_2 using a random key, while the other three are the output of a truly random permutation $f : \{0,1\}^{64} \to \{0,1\}^{64}$. All 64-bit outputs are encoded as 16 hex characters. Can you say which is the output of the PRP? Note that since you are able to distinguish the output of F_2 from random, F_2 is not a secure block cipher, which is what we wanted to show.

Hint: First argue that there is a detectable pattern in the xor of $F_2(\cdot, 0^{64})$ and $F_2(\cdot, 1^{32}0^{32})$. Then try to detect this pattern in the given outputs.

1. On input 0^{64} the output is "`5f67abaf 5210722b`". On input $1^{32}0^{32}$ the output is "`bbe033c0 0bc9330e`".

2. On input 0^{64} the output is "`2d1cfa42 c0b1d266`". On input $1^{32}0^{32}$ the output is "`eea6e3dd b2146dd0`".

3. On input 0^{64} the output is "`e86d2de2 e1387ae9`". On input $1^{32}0^{32}$ the output is "`1792d21d b645c008`".

4. On input 0^{64} the output is "`4af53267 1351e2e1`". On input $1^{32}0^{32}$ the output is "`87a40cfa 8dd39154`".

Question 5

Nonce-based CBC. Recall that in lecture 4.4 we said that if one wants to use CBC encryption with a non-random unique nonce then the nonce must first be encrypted with an independent PRP key and the result then used as the CBC IV. Let's see what goes wrong if one encrypts the nonce with the same PRP key as the key used for CBC encryption.

Let $F : K \times \{0,1\}^\ell \to \{0,1\}^\ell$ be a secure PRP with, say, $\ell = 128$. Let n be a nonce and suppose one encrypts a message m by first computing $IV = F(k, n)$ and then using this IV in CBC encryption using $F(k, \cdot)$. Note that the same key k is used for computing the IV and for CBC encryption. We show that the resulting system is not nonce-based CPA secure.

The attacker begins by asking for the encryption of the two block message $m = (0^\ell, 0^\ell)$ with nonce $n = 0^\ell$. It receives back a two block ciphertext (c_0, c_1). Observe that by definition of CBC we know that $c_1 = F(k, c_0)$. Next, the attacker asks for the encryption of the one block message $m_1 = c_0 \bigoplus c_1$ with nonce $n = c_0$. It receives back a one block ciphertext c'_0.

What relation holds between c_0, c_1, c'_0? Note that this relation lets the adversary win the nonce-based CPA game with advantage 1.

1. $c_1 = 0^\ell$

2. $c_1 = c_0 \bigoplus c'_0$

3. $c_1 = c'_0$

4. $c_0 = c_1 \bigoplus c'_0$

Question 6

Let m be a message consisting of ℓ AES blocks (say $\ell = 100$). Alice encrypts m using CBC mode and transmits the resulting ciphertext to Bob. Due to a network error, ciphertext block number $\ell/2$ 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?

Question 7

Let m be a message consisting of ℓ AES blocks (say $\ell = 100$). Alice encrypts m using randomized counter mode and transmits the resulting ciphertext to Bob. Due to a network error, ciphertext block number $\ell/2$ 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?

Question 8

Recall that encryption systems do not fully hide the length of transmitted messages. Leaking the length of web requests has been used to eavesdrop on encrypted HTTPS traffic to a number of web sites, such as tax preparation sites, Google searches, and healthcare sites. Suppose an attacker intercepts a packet where he knows that the packet payload is encrypted using AES in CBC mode with a random IV. The encrypted packet payload is 128 bytes. Which of the following messages is plausibly the decryption of the payload:

1. 'The most direct computation would be for the enemy to try all 2r̂ possible keys, one by one.'
2. 'If qualified opinions incline to believe in the exponential conjecture, then I think we cannot afford not to make use of it.'
3. 'We see immediately that one needs little information to begin to break down the process.'
4. 'In this letter I make some remarks on a general principle relevant to enciphering in general and my machine.'

Question 9

Let $R := \{0,1\}^4$ and consider the following PRF $F : R^5 \times R \to R$ defined as follows:

$$F(k,x) := \begin{cases} t = k[0] \\ \text{for i=1 to 4 do} \\ \qquad \text{if } (x[i-1] == 1) \quad t = t \oplus k[i] \\ \text{output } t \end{cases}$$

That is, the key is $k = (k[0], k[1], k[2], k[3], k[4])$ in R^5 and the function at, for example, 0101 is defined as $F(k, 0101) = k[0] \oplus k[2] \oplus k[4]$.

For a random key k unknown to you, you learn that

$$F(k, 0110) = 0011 \quad \text{and} \quad F(k, 0101) = 1010 \quad \text{and} \quad F(k, 1110) = 0110.$$

What is the value of $F(k, 1101)$? Note that since you are able to predict the function at a new point, this PRF is insecure.