Feedback — Week 2 - Problem Set

Help

You submitted this homework on **Tue 4 Feb 2014 9:30 PM PST**. You got a score of **9.00** out of **9.00**.

Question 1

Consider the following five events:

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.

What is the order of these events from most likely to least likely?

Your Answer		Score	Explanation
2, 3, 1, 4, 5			
2, 4, 3, 1, 5			
2, 3, 4, 1, 5	✔	1.00	• The probability of event (1) is 1/2^128. • The probability of event (5) is 1/(10^6)^7 which is about 1/2^{139}. Therefore, event (5) is the least likely. • The probability of event (4) is 1/(10^6)^6 which is about 1/2^{119.5} which is more likely than event (1). • The remaining events are all more likely than event (4).
2, 3, 5, 4, 1			
Total		1.00 / 1.00	

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 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.

Your Answer		Score	Explanation
More than a year but less than 100 years			
More than a month but less than a year			
More than a week but less than a month			
More than a billion (10^9) years	✔	1.00	The answer is about 540 billion years. • # machines = 4*10^12/200 = 2*10^10 • # keys processed per sec = 10^9 * (2*10^10) = 2*10^19 • # seconds = 2^128 / (2*10^19) = 1.7*10^19 This many seconds is about 540 billion years.
More than an hour but less than a day			
Total		1.00 / 1.00	

Question 3

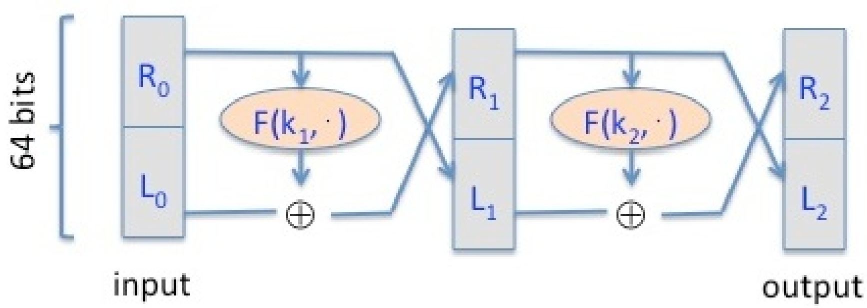
Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a secure PRF (i.e. a PRF where the key space, input space, and output space are all $\{0,1\}^n$) and say $n=128$. Which of the following is a secure PRF (there is more than one correct answer):

Your Answer		Score	Explanation
☐ $F'(k,\ x) = \begin{cases} F(k,x) & \text{when } x \neq 0^n \\ 0^n & \text{otherwise} \end{cases}$	✔	0.17	Not a PRF. A distinguisher will query at $x=0^n$ and output *not random* if the response is 0^n. This is unlikely to hold for a truly random function.
☐ $F'(k,x) = F(k,\ x) \bigoplus F(k,\ x \oplus 1^n)$	✔	0.17	Not a PRF. A distinguisher will query at $x=0^n$ and $x=1^n$ and output *not random* whenever the two responses are equal. This is unlikely to happen for a truly random function.
☑ $F'(k,x) = F(k,x)[0,\ldots,n-2]$ (i.e., $F'(k,x)$ drops the last bit of $F(k,x)$)	✔	0.17	Correct. A distinguisher for F' gives a distinguisher for F.
☐ $F'(k,\ x) = \begin{cases} F(k,x) & \text{when } x \neq 0^n \\ k & \text{otherwise} \end{cases}$	✔	0.17	Not a PRF. A distinguisher will query at $x=0^n$ and obtain k and then query at $x=1^n$ and output *not random* if the response is $F(k,1^n)$. This is unlikely to hold for a truly random function.
☑ $F'((k_1,k_2),\ x) = \begin{cases} F(k_1,x) & \text{when } x \neq 0^n \\ k_2 & \text{otherwise} \end{cases}$	✔	0.17	Correct. A distinguisher for F' gives a distinguisher for F.
☑ $F'((k_1,k_2),\ x) = F(k_1,x) \ \Big\|\ F(k_2,x)$ (here $\Big\|$ denotes concatenation)	✔	0.17	Correct. A distinguisher for F' gives a distinguisher for F.

Total	1.00 / 1.00

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.

Your Answer	Score	Explanation
○ On input 0^{64} the output is "9d1a4f78 cb28d863". On input $1^{32}0^{32}$ the output is "75e5e3ea 773ec3e6".		

(selected) On input 0^{64} the output is "e86d2de2 e1387ae9". On input $1^{32}0^{32}$ the output is "1792d21d b645c008".	✔	1.00	Observe that the two round Feistel has the property that the left of $F(\cdot, 0^{64}) \bigoplus F(\cdot, 1^{32}0^{32})$ is 1^{32}. The two outputs in this answer are the only ones with this property.
On input 0^{64} the output is "2d1cfa42 c0b1d266". On input $1^{32}0^{32}$ the output is "eea6e3dd b2146dd0".			
On input 0^{64} the output is "4af53267 1351e2e1". On input $1^{32}0^{32}$ the output is "87a40cfa 8dd39154".			
Total		1.00 / 1.00	

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 $F : K \times \{0,1\}^\ell \rightarrow \{0,1\}^\ell$ 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.

Your Answer		Score	Explanation
$c_1 = c_0'$	✔	1.00	This follows from the definition of CBC with an encrypted nonce as defined in the question.
$c_1 = c_0 \bigoplus c_0'$			
$c_0 = c_1 \bigoplus c_0'$			
$c_0' = c_0 \bigoplus 1^\ell$			
Total		1.00 / 1.00	

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?

Your Answer	Score	Explanation
3		
1		
ℓ		
$1 + \ell/2$		

2	✔	1.00	Take a look at the CBC decryption circuit. Each ciphertext blocks affects only the current plaintext block and the next.
Total		1.00 / 1.00	

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?

Your Answer		Score	Explanation
ℓ			
3			
2			
1	✔	1.00	Take a look at the counter mode decryption circuit. Each ciphertext block affects only the current plaintext block.
$1 + \ell/2$			
Total		1.00 / 1.00	

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:

Your Answer		Score	Explanation
'If qualified opinions incline to believe in the exponential conjecture, then I think we cannot afford not to make use of it.'			
'To consider the resistance of an enciphering process to being broken we should assume that at same times the enemy knows everything but the key being used and to break it needs only discover the key from this information.'			
'The significance of this general conjecture, assuming its truth, is easy to see. It means that it may be feasible to design ciphers that are effectively unbreakable.'			
'In this letter I make some remarks on a general principle relevant to enciphering in general and my machine.'	✔	1.00	The length of the string is 107 bytes, which after padding becomes 112 bytes, and after prepending the IV becomes 128 bytes.
Total		1.00 / 1.00	

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

$F(k, 0110) = 0011$ and $F(k, 0101) = 1010$ and $F(k, 1110) = 0110$.

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.

You entered:

1111

Your Answer		Score	Explanation
1111	✔	1.00	
Total		1.00 / 1.00	