Quiz 0920@znlady

Question 1

Winning a lottery with 1 million contestants_____(the biggest number) times in a row is easier than correctly guessing a random **256-bit** AES key on the first try.

Question 2

Suppose that using commodity hardware it is possible to build a computer for about $2000 that can brute force about 1 trillion 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, for 2016, US federal budget is $3.999 trillion). **How many years** 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.

Question 3

Let F be a secure pseudorandom function with 128-bit key and 256-bit block length. **Which** are the following functions G are secure pseudorandom generators? (Select all that apply.)

- $G(x)=F_x(0\ldots0)$, where x is a 128-bit input.
- $G(x)=F_x(0\ldots0)\,//\,F_x(0\ldots0)$, where x is a 128-bit input.
- $G(x)=F_x(0\ldots0)\,//\,F_x(1\ldots1)$, where x is a 128-bit input.
- $G(x)=F_{0\ldots0}(x)\,//\,F_{1\ldots1}(x)$, where x is a 256-bit input

Question 4

Say we use CBC-mode encryption based on a block cipher with 256-bit key length **and** 128-bit block length to encrypt a 512-bit message. **How long** is the resulting ciphertext?

Question 5.1

Let m be a message consisting of ℓ AES blocks (say ℓ=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 5.2

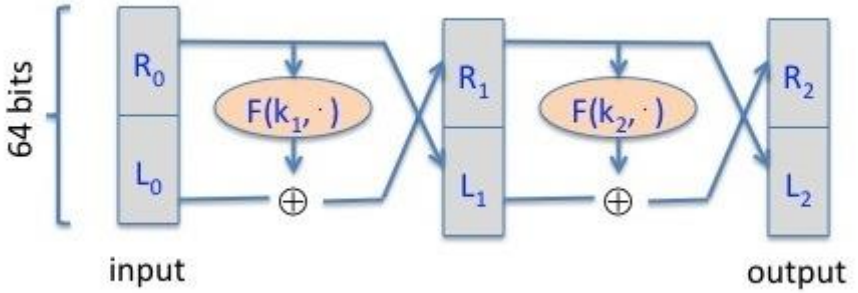
Let m be a message consisting of ℓ AES blocks (say ℓ=100). Alice encrypts m using randomized **counter mode** and transmits the resulting ciphertext to Bob. Due to a network error, ciphertext block number $\ell/2$ is corrupted during transmission. All other ciphertext blocks are transmitted and received correctly. Once Bob decrypts the received ciphertext, **how many** plaintext blocks will be corrupted?

Question 6

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. **Construct** at least 3 secure PRF with ***F.*** **(try your best)**

Question 7

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. **Prove** that a **two** round Feistel cannot give a secure block cipher.



Let F: $K \times \{0,1\}^{32} \rightarrow \{0,1\}^{32}$ be a secure PRF. Recall that a 2-round Feistel defines the following PRP F_2: $K^2 \times \{0,1\}^{64} \rightarrow \{0,1\}^{64}$:

Hint: give a counterexample say that F_2 is not a secure block cipher

Question 8

Let R:={0,1}^{4}and consider the following PRF F: $R^5 \times R \rightarrow R$ defined as follows: **Prove** that this PRF is insecure.

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

Solution to Quiz 00912@znlady

Question 1

Assume an honest user wants to send an 8-bit integer to their bank indicating how much money should be transferred to the bank account of an attacker. The user uses **CTR-mode** encryption based on a block cipher F with 8-bit block length. (Yes, this is a made-up example.) The attacker knows that the amount of money the user wants to transfer is exactly **$16**, and has compromised a router between the user and the back. The attacker receives the ciphertext 10111100 01100001 (in binary) from the user. **What ciphertext** should the attacker forward to the bank to initiate a transfer of exactly **$32**? (Recall that CTR-mode decryption of a ciphertext c_0, c_1 using key k is done by outputting $c_1 \oplus F_k(c_0+1)$.) 10111100 01010001

Question 2

Assume CTR-mode encryption with PKCS #5 padding and a block cipher with 8-byte block length. Say a 4-byte message is encrypted, resulting in ciphertext 0x00 01 02 03 04 05 06 07 00 01 02 03 04 05 06 07. **Which** of the following ciphertexts will NOT yield an error upon decryption?

0x00 01 02 03 04 05 06 07 00 01 02 03 05 05 06 07

0x00 01 02 03 04 05 06 07 00 01 02 03 04 05 07 07

0x00 01 02 03 04 05 06 07 00 01 02 04 04 05 06 07

0x00 01 02 03 04 05 06 07 00 01 02 03 04 05 06 F7