西安電子科技大學
XIDIAN UNIVERSITY

Week 2 - Problem Set

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?

   - ○ 3, 2, 5, 4, 1
   - ○ 2, 3, 4, 1, 5
   - ○ 2, 3, 1, 5, 4
   - ○ 2, 3, 5, 4, 1

1） $1/2^{128} \approx 1/10^{38}$

2） $1/10^{6}$

3） $1/10^{30}$

4） $1/10^{36}$

5） $1/10^{42}$

2>3>4>1>5

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.

- ○ More than a month but less than a year
- ○ More than a billion (10^9) years
- ○ More than a year but less than 100 years
- ○ More than a week but less than a month
- ○ More than a 100 years but less than a million years

西安电子科技大学 XIDIAN UNIVERSITY

$4 \times 10^{12} / 200 = 2 \times 10^{10}$台电脑

$2 \times 10^{10} \times 10^{9} = 2 \times 10^{19}$ 比特每秒

$2^{128} / 2 \times 10^{19} \approx 10^{38} / 2 \times 10^{19} = 5 \times 10^{18}$秒

5×10^{18}秒$\approx 1.6 \times 10^{11}$年

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):

- [ ] $F'(k,x) = F(k,x) \parallel 0$

  (here $\parallel$ denotes concatenation)

- [ ] $F'(k,x) = F(k,x)[0,\ldots,n-2]$

  (i.e., $F'(k,x)$ drops the last bit of $F(k,x)$)

- [ ] $F'(k,x) = F(k,\ x) \bigoplus F(k,\ x \oplus 1^n)$

- [ ] $F'((k_1,k_2),\ x) = \begin{cases} F(k_1,x) & \text{when } x \neq 0^n \\ k_2 & \text{otherwise} \end{cases}$

- [ ] $F'(k,\ x) = k \bigoplus x$

- [ ] $F'((k_1,k_2),\ x) = F(k_1,x) \parallel F(k_2,x)$ (here $\parallel$ denotes concatenation)

4. Recall that the Luby-Rackoff theorem discussed in The Data Encryption Standard lecture 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

   $F_2: K^2 \times \{0,1\}^{64} \to \{0,1\}^{64}$:

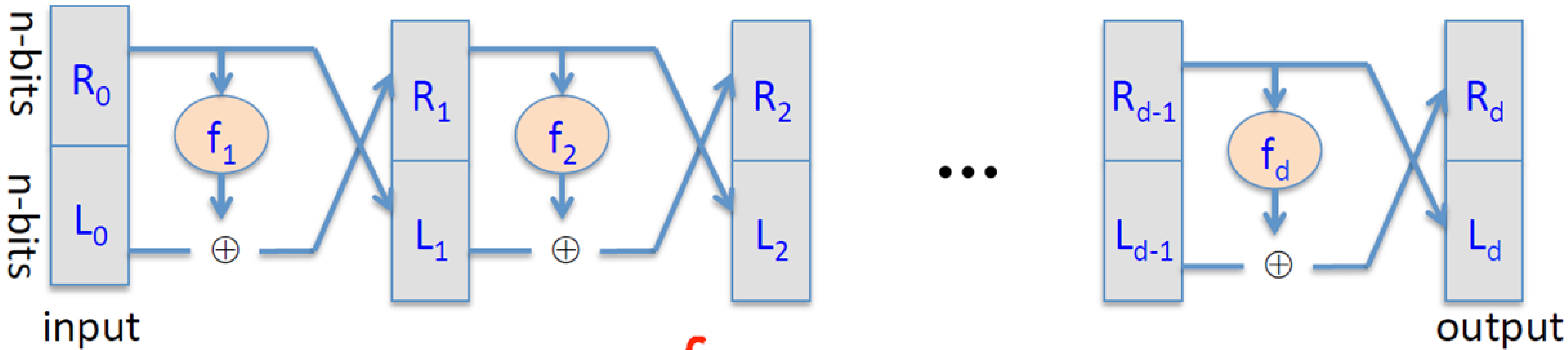
   Here R_0 is the right 32 bits of the 64-bit input and L_0 is the left 32 bits.

   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.

   - On input 0^{64} the output is "e86d2de2 e1387ae9".
     On input $1^{32}0^{32}$ the output is "1792d21d b645c008".
   - On input 0^{64} the output is "5f67abaf 5210722b".
     On input $1^{32}0^{32}$ the output is "bbe033c0 0bc9330e".
   - On input 0^{64} the output is "7c2822eb fdc48bfb".
     On input $1^{32}0^{32}$ the output is "325032a9 c5e2364b".
   - On input 0^{64} the output is "7b50baab 07640c3d".
     On input $1^{32}0^{32}$ the output is "ac343a22 cea46d60".



In symbols: $\begin{cases} R_i = f_i(R_{i-1}) \oplus L_{i-1} \\ L_i = R_{i-1} \end{cases}$

$R_1=F(R_0) \oplus L_0$
$L_1=R_0$

$R_2=F(F(R_0) \oplus L_0) \oplus R_0$
$L_2=F(R_0) \oplus L_0$

令$L_0=0^{32}, R_0=0^{32}$,可得$L_2=F(0^{32}) \oplus 0^{32}$

令$L_0=1^{32}, R_0=0^{32}$,可得$L_2=F(0^{32}) \oplus 1^{32}$

$F(0^{32}) \oplus 0^{32} \oplus F(0^{32}) \oplus 1^{32} = 1^{32}$

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 $c_1 = F(k, c_0)$.

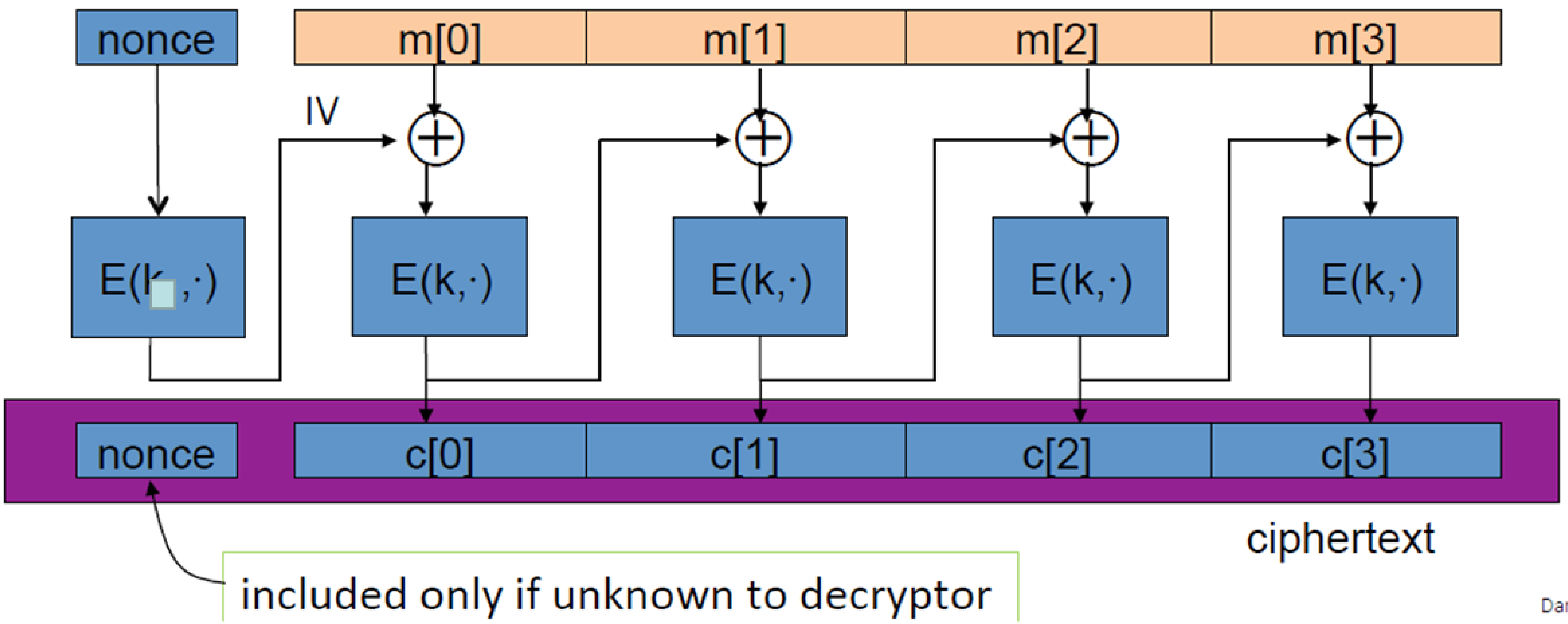
Next, the attacker asks for the encryption of the one block message $m_1 = c_0 \bigoplus c_1$ with nonce $n = c_0$. It receives back a one block ciphertext c_0'.

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.

- ○ $c_0' = c_0 \bigoplus 1^\ell$
- ○ $c_1 = c_0'$
- ○ $c_0 = c_1 \bigoplus c_0'$
- ○ $c_1 = c_0 \bigoplus c_0'$

0^{128} 0^{128} 0^{128} $\Rightarrow c_1 = E(k, c_0)$

c_0 $c_0 \oplus c_1$ $\Rightarrow c_0' = E(k, (c_0 \oplus c_1 \oplus E(k, c_0))) = c_1$



Dan Boneh

西安电子科技大学
XIDIAN UNIVERSITY

6. Let m be a message consisting of ℓ AES blocks

(say $\ell = 100$). Alice encrypts m using $\boxed{\text{CBC mode}}$ and transmits

the resulting ciphertext to Bob. Due to a network error,

$\boxed{\text{ciphertext block number } \ell/2 \text{ is corrupted during transmission.}}$

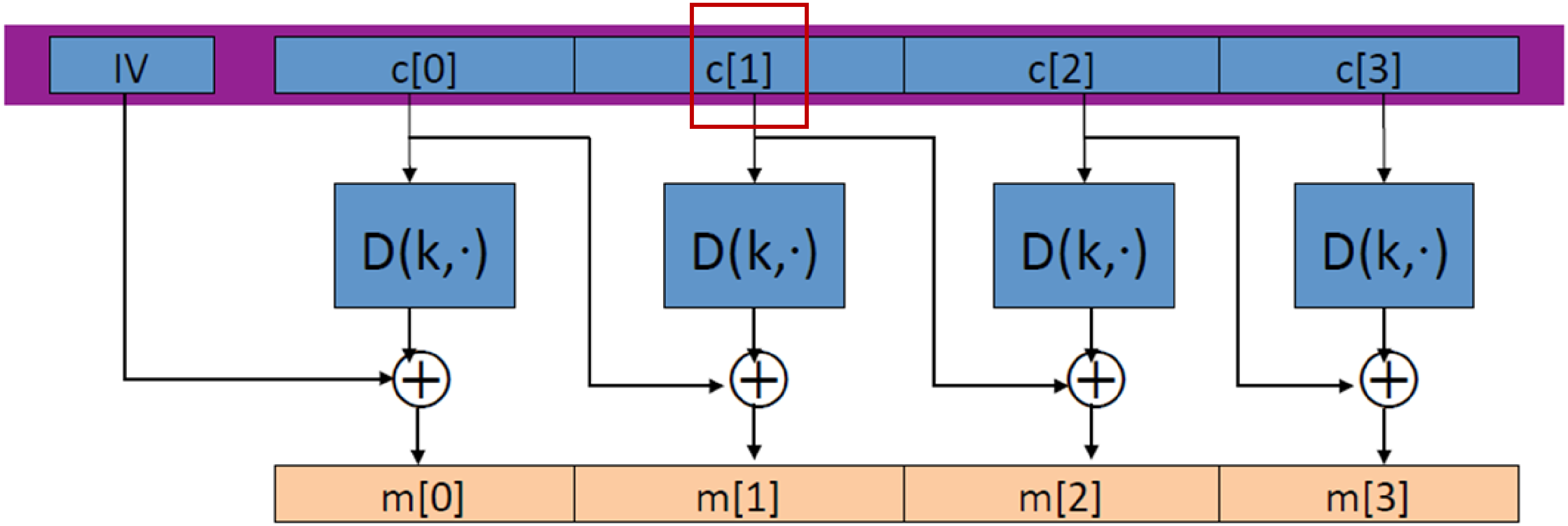
All other ciphertext blocks are transmitted and received correctly.

Once Bob decrypts the received ciphertext, how many plaintext blocks

will be corrupted?

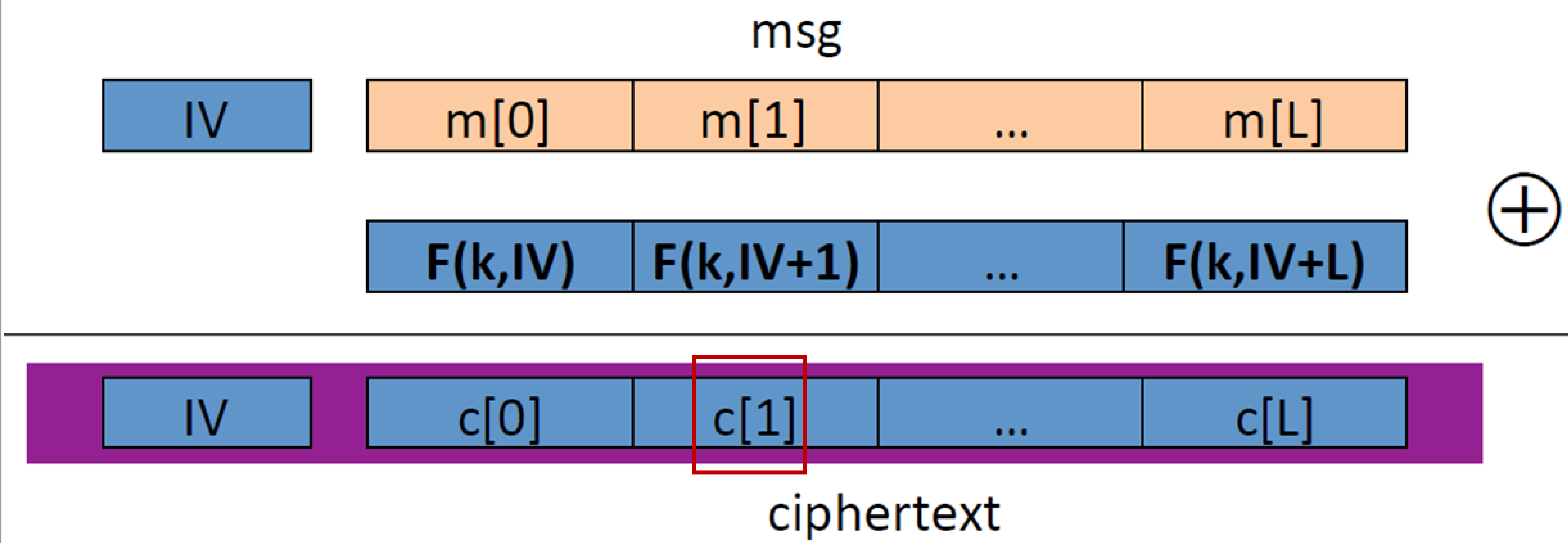
- ◯ 2
- ◯ $1 + \ell/2$
- ◯ $\ell/2$
- ◯ 1
- ◯ 0

假设c[1]出错



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?

- ◯ $\ell/2$
- ◯ 0
- ◯ ℓ
- ◯ 2
- ◯ 1



假设c[1]出错

8. Recall that encryption systems do not fully hide the **length** of

transmitted messages. Leaking the length of web requests [hasbeen 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:

165bytes
- ○ '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.'

124bytes
- ○ 'If qualified opinions incline to believe in the exponential conjecture, then I think we cannot afford not to make use of it.'
- ○ 'In this letter I make some remarks on a general principle relevant to enciphering in general and my machine.'

108
+ padding=112 (16×7)
+ IV =128

92bytes
- ○ 'The most direct computation would be for the enemy to try all 2^r possible keys, one by one.'

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

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

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.

$$F(k, 0110) = k[0] \oplus k[2] \oplus k[3]$$
$$= 0011$$
$$F(k, 0101) = k[0] \oplus k[2]$$
$$\oplus k[4] = 1010$$
$$F(k, 1110) = k[0] \oplus k[1] \oplus k[2] \oplus k[3]$$
$$= 0110$$

$$F(k, 1101) = k[0] \oplus k[1] \oplus k[2]$$
$$\oplus k[4]$$
$$= F(k, 0110) \oplus$$