

# Cryptography CS 555



## Review of Mid-term Exam & HW's

# Problem 1a: Classical Ciphers

- What is the index of coincidence of the 10-character word "cryptology"?

$$I_C(\text{"cryptology"}) = \frac{\sum_{i=0}^{25} \binom{f_i}{2}}{\binom{10}{2}} = \frac{\sum_{i=0}^{25} \frac{f_i(f_i-1)}{2}}{\frac{10 \cdot 9}{2}} = \frac{2}{45} = 0.044$$

# Problem 1b: Classical Ciphers

- What is the most effective ciphertext only attack against the shift cipher?
  - exhaustive key search, frequency analysis
- What is the most effective ciphertext only attack against the substitution cipher?
  - frequency analysis
- What is the most effective known plaintext attack against the substitution cipher?
  - directly compute key (or first computer key and then frequency analysis)

# Problem 1b

- What is the most effective known plaintext attack against the Rotor machine cipher?
  - exhaustive key search
- What is the most effect chosen plaintext attack against the Vigenere cipher?
  - direct compute key
- What is the most effective chosen plaintext attack against the Rotor machine cipher?
  - exhaustive key search, direct compute key

# Problem 2a

- Are the following statements correct?
  - For any cipher that has perfect secrecy, the keyspace and the ciphertext space must have the same size.
    - Answer: no.
  - For any cipher that has perfect secrecy, the size of the plaintext space must be greater than the size of the keyspace.
    - Answer no.

# Problem 2c

- Part b and c: yes. Look at Part c.
- Key observation: Given any ciphertext  $j$ , the probability that  $a$  is encrypted to  $j$  is the same as the probability that  $b$  is encrypted to  $j$ .
- It doesn't matter that the ciphertext 3 may occur less frequently than other ciphertexts.
- More formally, given any Prob. Dist. for plaintexts

$$\begin{aligned}\Pr[ P = a \mid C = 1 ] &= \frac{\Pr[ P = a ] \Pr[ C = 1 \mid P = a ]}{\Pr[ C = 1 ]} \\ &= \frac{\Pr[ P = a ] \cdot \frac{2}{5}}{\Pr[ P = a ] \cdot \frac{2}{5} + \Pr[ P = b ] \cdot \frac{2}{5}} = \Pr[ P = a ]\end{aligned}$$

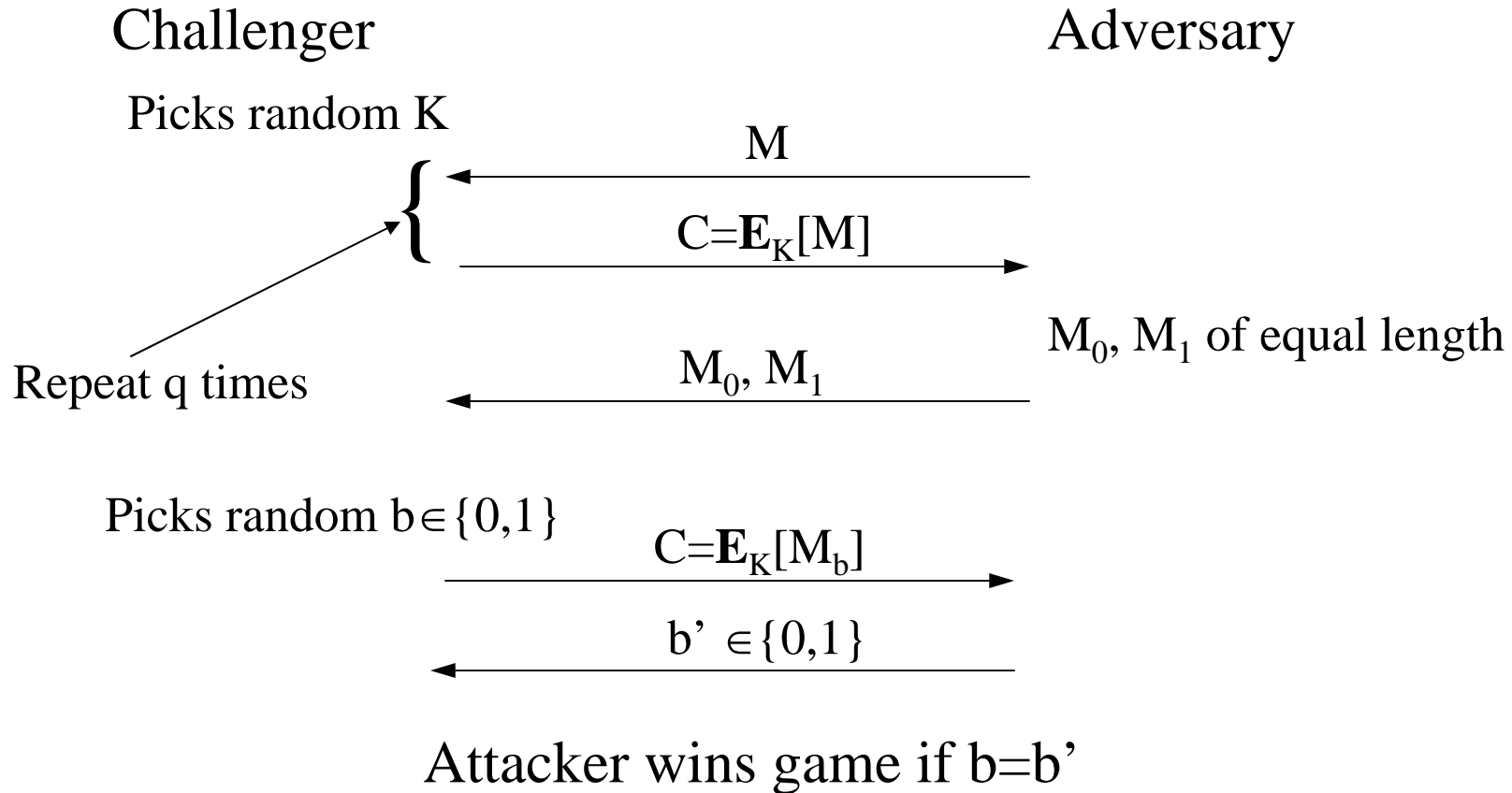
# Problem 3

- Given a 3-stage LFSR, which is described as  $s_i = s_{i-1} \oplus s_{i-2}$ , for  $i \geq 3$ . Suppose that we have observed that  $s_4 = 1$ ,  $s_5 = 1$ ,  $s_6 = 0$ , what is the internal state  $s_0, s_1, s_2$ .
  - We know that the sequence will repeat:
  - $s_0 \ s_1 \ s_2 \ s_3 \ s_4 \ s_5 \ s_6 \ s_7 \ s_8 \ s_9$   
                                  1 1 0 1 1 0  
                                  ? 1 1 0
  - Direct solution also works

# Problem 4

- During the transmission of a 640-bit ciphertext, bit 203 is flipped.
  - How many bits MAY be incorrect after decryption using ECB
    - Answer: one block, 64 bits
  - CBC
    - $M_i = C_{i-1} \oplus D_K[C_i]$        $M_{i+1} = C_i \oplus D_K[C_{i+1}]$
    - Answer: 65
  - CTR
    - $M_i = C_i \oplus E_K[\text{counter}]$
    - Answer: 1

# Problem 5a: IND-CPA



# Problem 5b: Attacking CBC with fixed

- CBC:  $C_1 = IV \oplus E_K[M_1]$ 
  - fixed IV implies that first cipher block will ,
- The adversary does the following
  - let  $B_0$  and  $B_1$  be two different blocks,
  - training: sends  $M = B_0B_1$  and receives  $C_0C_1$
  - sends  $(B_0B_0, B_1B_1)$  and receives  $C_0'C_1'$
  - return 0 if  $C_0 = C_0'$  and 1 otherwise

# Problem 6a: Variation of 3DES

- $3DES_{K_1, K_2}[M] = E_{K_1}[D_{K_2}[E_{K_1}[M]]]$
- Given  $(M_1, C_1)$ , compute number of expecting key pairs encrypting  $M_1$  into  $C_1$ 
  - there are  $2^{64}$  possible blocks that  $M_1$  could be encrypted into, each one is equally likely. There are  $(2^{56})^2$  possible key pairs, so the answer is  $2^{112-64} = 2^{48}$

# Problem 6b

- Given two pairs, compute number of expecting key pairs consistent with them
  - there are  $(2^{64})^2$  possible outcomes for encrypting both  $M_1$  and  $M_2$ , each one is equally likely.
  - There are  $(2^{56})^2$  possible key pairs, so the answer is  $2^{112-128}=2^{-16}$

# Problem 6c:

- We have  $T_K = 3DES_{K1,K2}[D_K[B_0]]$   
 $= E_{K1}[D_{K2}[E_{K1}[D_K[B_0]]]]$
- If  $K$  happens to be  $K1$ , then  $T_K = E_K[D_{K2}[B_0]]$ ,
  - we need to find  $K2$ , and we have a table mapping  $D_K[B_0]$  to  $K$  for every  $K$ , what to do?
  - note  $T_K = E_K[D_{K2}[B_0]]$  is equivalent to  $D_K[T_K] = D_{K2}[B_0]$
- we compute  $D_K[T_K]$  and then look up the  $K2$  in the table. If we find it (what is the probability?), then we have a pair that we can see whether its correct using  $(M_1, C_1)$  and  $(M_2, C_2)$

# Problem 6

- Time complexity
  - building table:  $2^{56}$
  - for each key, we do constant time operation
  - total complexity is  $2^{56}$
- It is theoretically better than exhaustive key search, but this is not practical, as we need  $2^{57}$  chosen plaintext queries

# Problem 7b

- Show that if either  $h_1$  or  $h_2$  is a weakly collision resistant hash function, then  $h(x)=h_1(x)||h_2(x)$  is also a weakly collision resistant hash function.
- Proof: If  $h(x)$  is not weakly collision resistant, then there is an algorithm that can given  $x$  output  $x'$  such that  $h(x)=h(x')$ , which means that  $h_1(x)=h_1(x')$  and  $h_2(x)=h_2(x')$ . The same algorithm thus can also find 2<sup>nd</sup>-preimage for  $h_1$  and for  $h_2$ , thus, neither  $h_1$  nor  $h_2$  is weakly collision resistant.

# Problem 8a

- $h_K(x_1, \dots, x_n) = E_K(x_1) \oplus \dots \oplus E_K(x_n) \quad n \geq 2$ 
  - a. choose  $x_1 \neq x_n$ , asks for  $c = h_K(x_1, x_2, \dots, x_n)$ , output  $(x_2, x_1, \dots, x_n), c$
  - b. when given a message  $(x_1, \dots, x_n)$ , if there are two blocks that are different, then swap them and request the MAC. If the message is  $(x, x, \dots, x)$ , then when  $n$  is even, the MAC is 0. When  $n$  is odd, request MAC for  $(x', x', x, \dots, x)$ , which is also the MAC for the requested message.

# Problem 9

- Compute  $5^{179} \pmod{19}$ 
  - Little Fermat Theorem:  $a^{p-1} \pmod{p} = 1$ , when  $\gcd(a,p)=1$
  - $a^{18} \pmod{19} = 1$
  - $a^{180} \pmod{19} = 1$
  - $a^{179} = a^{180-1} = a^{-1} = 4 \pmod{19}$

# Problem 9b

- Prove that  $\phi(n)$  is even for  $n > 2$ 
  - if  $n$  has an odd prime factor  $p$ , let  $n = p^e m$  such that  $\gcd(p, m) = 1$ , then  $\phi(n) = \phi(p^e)\phi(m) = (p^e - p^{e-1})\phi(m)$ , as  $p$  is odd, both  $p^e$  and  $p^{e-1}$  are odd, and  $(p^e - p^{e-1})$  is even,  $\phi(n)$  is thus even
  - if  $n$  has no odd prime factor, then  $n = 2^k$  and  $k \geq 2$ ,  $\phi(n) = 2^k - 2^{k-1} = 2^{k-1}$ , as  $k-1 \geq 1$ ,  $2^{k-1}$  is even

# Problem 10a

- $F_K[M] = (E_K[R], R \oplus M)$
- KR-RPA against  $E_K$

Challenger

Adversary

Picks random  
 $K, M_1, \dots, M_q$

$(M_i, C_i = E_K[M_i])$  for  $1 \leq i \leq q$

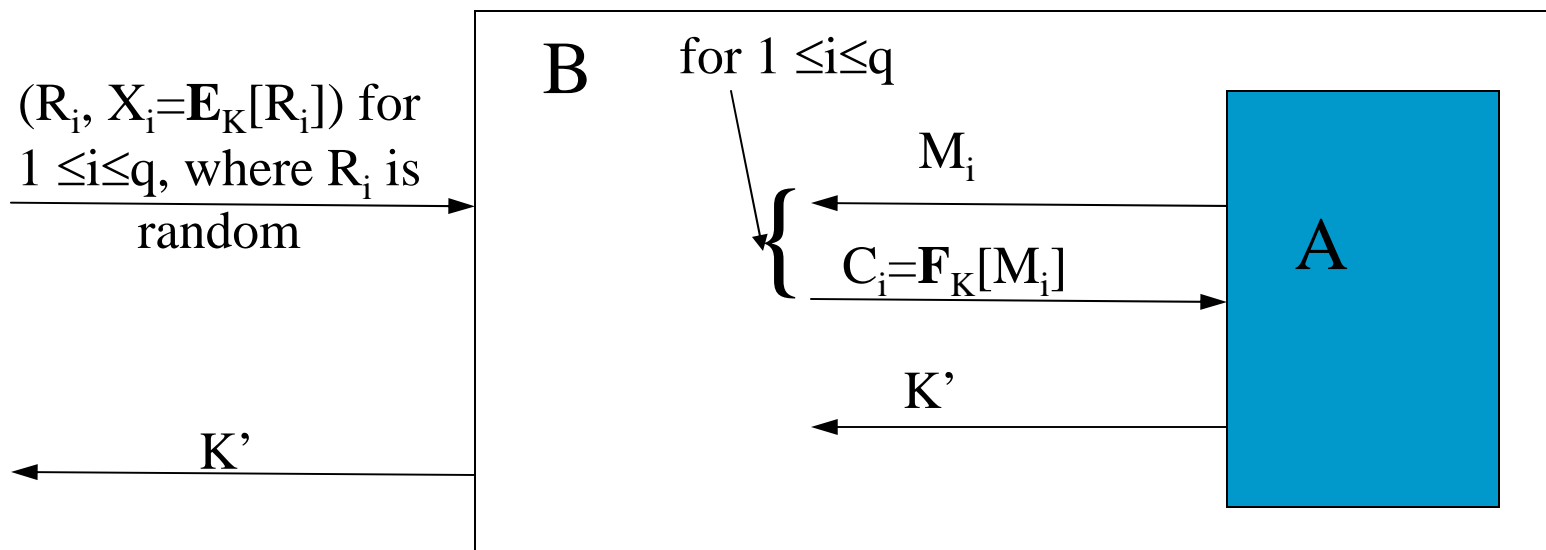
$K'$

Attacker wins game if  $K = K'$



# Problem 10c

- Prove that if  $E_K$  is secure against KR-RPA, then  $F_K$  is secure against KR-CPA
- Suppose that  $A$  breaks KR-CPA against  $F_K$ , we now build  $B$  that breaks KR-RPA of  $E_K$ .



# Assignment 2: Problem 1

- Consider the following insecure PRNG: Given prime  $p$  and  $a, b, c$ , the seed is  $(s_1, s_2)$ 
  - output  $(cx_1+x_2)$  when  $(x_1, x_2)$  is internal state
  - set new state to  $(ax_1+x_2, bx_2+x_1) \bmod p$
- let  $y_1, y_2$  be two outputs
  - $x_1=s_1, x_2=s_2, \quad y_1=cs_1+s_2$
  - $x_1=as_1+s_2, x_2=bs_2+s_1, \quad y_2=c(as_1+s_2)+bs_2+s_1,$
  - $y_2=c(as_1+y_1-cs_1)+b(y_1-cs_1)+s_1$
  - $(ca-c+bc+1)s_1=y_2-cy_1+by_1$

# To be finished

# Next ...

- RSA
- Prime number distribution and testing
- Efficiency of modular arithmetic

