

# Set of Problems 1

Dr. Arjan Duresi  
Louisiana State University  
Baton Rouge, LA 70810  
Duresi@csc.LSU.Edu

These slides are available at:

[http://www.csc.lsu.edu/~duresi/CSC4601\\_07/](http://www.csc.lsu.edu/~duresi/CSC4601_07/)

# Problem 1

1.[10 points] Assume a cryptographic algorithm in which the performance for the good guys (the one that know the key) grows linearly with the length of the key, and for which the only way to break it is by brute-force attack of trying all possible keys. Suppose the performance of the good guys is adequate (e.g. it can encrypt and decrypt as fast as the bits can be transmitted over the wire) at a certain key size. Then suppose advances in computer technology make computers twice as fast. Given that both the good guys and the bad ones get faster computers, does this advance in computer speed work to the advantage of the good guys, the bad guys, or doesn't make any difference?

# Problem 1 - Solution

If the good guys keep the same size key, than it is an advantage for bad guys. But if the good guys double the key size, doubling their work while still taking the same amount of time as it used to, than it's much worse for the bad guys, since their work squares.

## Problem 2

2. [7 points] Suppose A, B and C use  $K_a$ ,  $K_b$ , and  $K_c$  as corresponding secret keys for authentication. So each one of them responds to a challenge with the encrypted challenge. Is this more secure than having them all use the same key?

# Problem 2 - Solution

No, because they still have to share the keys.

## Problem 3

3. [7 points] Let's assume you do DES double encryption by encrypting with  $K_1$  and decrypting with  $K_2$ . Does the same attack work as with double encryption with  $K_1$  and  $K_2$ ?

# Problem 3 - Solution

Yes, from the security point of view is the same thing.

## Problem 4

4. [7 points] Message digests are reasonable fast, but here's a much faster function to compute. Take your message, divide it into 128-bit chunks, and  $\oplus$  all chunks together to get a 128-bit result. Then do the standard message digest on the result. Is this a good message digest function?

# Problem 4 - Solution

No, it is fairly easy to generate another message with the same 128-bit  $\oplus$ .

## Problem 5

5. [7 points] Assume a good 128-bit message digest function. Assume there is a particular value,  $d$ , for the message digest and you'd like to find a message that has a message digest of  $d$ . Given that there are many more 2000-bit messages that map to a particular 128-bit message digest than 1000-bit messages, would you theoretically have to test fewer 2000-bit messages to find one that has a message digest of  $d$  than if you were to test 1000-bit messages?

# Problem 5 - Solution

No. The expected number of messages you'd need to try is  $2^{128}$  in either case.

# Problem 6

6. [10 points] What are two problems with one-time pad?

# Problem 6 - Solution

- ❑ To generate random pads
- ❑ To distribute them

# Problem 7

- ❑ 7. Multi choice and True or false? (Grading: +1 for each correct answer. -1 for each incorrect answer. 0 for no answer)
- ❑ 1. The essential ingredients of a symmetric cipher are\_\_\_\_\_
- ❑ a) Plaintext and ciphertext, algorithm.
- ❑ b) encryption and decryption algorithms
- ❑ c) secret key,
- ❑ d) all of the above

# Problem 7 - Solution

□ d

## Problem 8

- ❑ 2. An encryption scheme is said to be computationally secure if \_\_\_\_\_
- ❑ a) the cost of breaking the cipher exceeds the value of the encrypted information.
- ❑ b) the time required to break the cipher exceeds the useful lifetime of the information.
- ❑ c) the algorithm is unknown
- ❑ d) all of the above

# Problem 8 - Solution

□ a, b

# Problem 9

- ❑ 3. Which parameters and design choices determine the strength of DES cipher? \_\_\_\_\_
- A) Block size
  - B) Key size
  - C) Number of rounds
  - D) Initial permutation
  - E) Subkey generation algorithm
  - F) Round function
  - G) Ease of analysis

# Problem 9 - Solution

- a, b, c, e, f, g

# Problem 10

One way to protect Diffie-Hellman against the Man-in-the-Middle attack is to encrypt the Diffie-Hellman value with the other side's public key. Why is this the case, given that an attacker can encrypt whatever it wants with the other side's public key?

# Problem 10 - Solution

The attacker will not be able to decrypt the Diffie-Hellman values sent to him and so will not be able to compute the shared secrets.

# Problem 11

- Each node  $N$  of a network is been assigned a unique secret key  $K_n$ . This key is used to secure communications between the node and a trusted server. That is, all the keys are stored on a server. User  $A$ , wishing to send a secret message  $M$  to user  $B$ , initiates the following protocol:
  1.  $A$  generates a random number  $R$  and sends to the server his name  $A$ , destination  $B$ , and  $E_{K_a}[R]$
  2. Server responds by sending  $E_{K_b}[R]$  to  $A$
  3.  $A$  sends  $E_R[M]$  together with  $E_{K_b}[R]$  to  $B$ .
  4.  $B$  knows  $K_b$ , thus decrypts  $E_{K_b}[R]$  to get  $R$  and will subsequently use  $R$  to decrypt  $E_R[M]$  to get  $M$ .
- Analyze this protocol. Is it safe?

# Solution Problem 11

- ❑ The protocol is not secure. The server doesn't authenticate the sender. So an intruder Z can intercept  $E_{K_a}[R]$  and  $E_R[M]$ .
- ❑ Then Z sends to the server the source name A, the destination name Z (his own), and , as if A wanted to send him the same message encrypted under the same key R as A did it with B.
- ❑ The server will respond by sending  $E_{K_z}[R]$  to A and Z will intercept that
- ❑ Because Z knows his key  $K_z$ , he can decrypt  $E_{K_z}[R]$ , thus getting his hands on R that can be used to decrypt  $E_R[M]$  and obtain M.

# Problem 12

□ 5. [10 points] A simple protocol based on public key works as follows.

1. A sends to B  $(A, EK_{U_b}[M, A], B)$
2. B acknowledges receipt by sending to A  $(B, EK_{U_a}[M, B], A)$

To avoid the redundancy of the above protocol a second protocol was proposed:

1. A sends to B  $(A, EK_{U_b}[M], B)$
2. B acknowledges receipt by sending to A  $(B, EK_{U_a}[M], A)$

□ Is the second protocol secure? Describe a possible attack on it

# Problem 12 - Solution

- Z can capture the message  $A \rightarrow B$  and send it to B as:  
(Z,  $E_{K_{Ub}}[M]$ , B)

# Problem 13

4.   Permutation and substitution are the two basic functions used in encryption algorithms.
5.   One key is required for two people to communicate via an asymmetric ciphers.
6.   A block cipher is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.
7.   . An encryption scheme is unconditionally secure if the ciphertext generated by the scheme contains enough information to determine uniquely the corresponding plaintext, no matter how much ciphertext is available.
8.   The Caesar cipher involves replacing each letter of the alphabet with the letter standing  $k$  places further down the alphabet, for  $k$  in the range 1 through 25.
9.   A polyalphabetic substitution cipher maps a plaintext alphabet to a ciphertext alphabet, so that each letter of the plaintext alphabet maps to a single unique letter of the ciphertext alphabet.
10.   A stream cipher is one that encrypts a digital data stream one bit or one byte at a time..
11.   A transposition cipher involves a permutation of the plaintext letters.

# Problem 13 Solutions

4. ✓  Permutation and substitution are the two basic functions used in encryption algorithms.
5.  ✓ One key is required for two people to communicate via an asymmetric ciphers.
6. ✓  A block cipher is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.
7.  ✓ . An encryption scheme is unconditionally secure if the ciphertext generated by the scheme contains enough information to determine uniquely the corresponding plaintext, no matter how much ciphertext is available.
8. ✓  The Caesar cipher involves replacing each letter of the alphabet with the letter standing  $k$  places further down the alphabet, for  $k$  in the range 1 through 25.
9.  ✓ A polyalphabetic substitution cipher maps a plaintext alphabet to a ciphertext alphabet, so that each letter of the plaintext alphabet maps to a single unique letter of the ciphertext alphabet.
10. ✓  A stream cipher is one that encrypts a digital data stream one bit or one byte at a time..
11. ✓  A transposition cipher involves a permutation of the plaintext letters.

# Problem 14

12.   Steganography involves concealing the existence of a message.
13.   Most asymmetric block encryption algorithms in current use are based on the Feistel block cipher structure..
14.   The S-box is a substitution function that introduces nonlinearity and adds to the complexity of the transformation.
15.   The avalanche effect is a property of any encryption algorithm such that a small change in either the plaintext or the key produces a significant change in the ciphertext.
16.   In all modes, the plaintext does not pass through the encryption function, but is XORed with the output of the encryption function.
17.   Usually triple encryption (3DES) is used with three distinct keys for the three stages .
18.   3DES consist in three stages of encryption.
19.  . Linear cryptanalysis is based on finding linear approximations to describe the transformations performed in a block cipher.
20.   Differential cryptanalysis is a technique in which chosen plaintexts with particular XOR difference patterns are encrypted. The difference patterns of the resulting ciphertext provide information that can be used to determine the encryption key
21.   A monoalphabetic substitution cipher uses a separate monoalphabetic substitution cipher for each successive letter of plaintext, depending on a key.
22.   In confusion, the statistical structure of the plaintext is dissipated into long range statistics of the ciphertext. This is achieved by having each plaintext digit affect the value of many ciphertext digits, which is equivalent to saying that each ciphertext digit is affected by many plaintext digits.

# Problem 14 Solutions

- 12. ✓  Steganography involves concealing the existence of a message.
- 13.  ✓ Most asymmetric block encryption algorithms in current use are based on the Feistel block cipher structure..
- 14. ✓  The S-box is a substitution function that introduces nonlinearity and adds to the complexity of the transformation.
- 15. ✓  The avalanche effect is a property of any encryption algorithm such that a small change in either the plaintext or the key produces a significant change in the ciphertext.
- 16.  ✓ In all modes, the plaintext does not pass through the encryption function, but is XORed with the output of the encryption function.
- 17.  ✓ Usually triple encryption (3DES) is used with three distinct keys for the three stages .
- 18.  ✓ 3DES consist in three stages of encryption.
- 19. ✓ . Linear cryptanalysis is based on finding linear approximations to describe the transformations performed in a block cipher.
- 20. ✓  Differential cryptanalysis is a technique in which chosen plaintexts with particular XOR difference patterns are encrypted. The difference patterns of the resulting ciphertext provide information that can be used to determine the encryption key
- 21.  ✓ A monoalphabetic substitution cipher uses a separate monoalphabetic substitution cipher for each successive letter of plaintext, depending on a key.
- 22.  ✓ In confusion, the statistical structure of the plaintext is dissipated into long range statistics of the ciphertext. This is achieved by having each plaintext digit affect the value of many ciphertext digits, which is equivalent to saying that each ciphertext digit is affected by many plaintext digits.