Information Systems Security: exercises on foundational techniques for cybersecurity

Diana Berbecaru

< diana.berbecaru @ polito.it >

Politecnico di Torino

Dip. Automatica e Informatica

AA 2023-2024

Outline

- **questions (multiple-choice)**
  - part 1: symmetric crypto
  - part 2: asymmetric crypto
- **exercises**

Questions
(Part 1)

Question 1

- **DES is an algorithm that allows:**
  - A. symmetric encryption of data by splitting data in blocks
  - B. symmetric encryption of data by processing the data flow
  - C. creation of digital signatures with asymmetric keys
  - D. creation of digital signature and encryption of data with asymmetric keys

Question 2

- **The key length to defend from brute force attacks has increased because**
  - A. the use of permutations and transpositions in algorithms has increased
  - B. as algorithms get stronger, they get less complex, and thus more susceptible to attacks
  - C. processor speed and power have increased
  - D. key length reduces over time

Question 3

- **What of the following properties should a secure AES key have?**
  - A. confidentiality
  - B. non-repudiation
  - C. traceability
  - D. randomness

Question 4

- **The advantages of the ECB mode are:**
  - A. parallel encryption
  - B. parallel decryption
  - C. random access to blocks (you can decrypt a block independently from the others)
  - D. simple implementation
  - E. difficult to perform cryptanalysis because identical blocks encrypt differently
  - F. it's not possible to swap blocks
  - G. it's not possible to delete blocks
  - H. is resistant to known-plaintext attacks

Question 5

- **if a tool uses AES-256-ECB, you can assume that**
  - A. the tool can accept as a possible input either a private key or a public key
  - B. the tool will have a negligible padding size
  - C. the tool will operate on an Initialization Vector of 128 bit
  - D. the tool adopts a symmetric algorithm, with a 256-bit key, and where each block of ciphertext is related to only one block of plaintext

Question 6

- **Which of the following statements are true for the CBC mode?**
  - A. parallel decryption
  - B. parallel encryption
  - C. protection on order of blocks
  - D. if one cyphertext block is lost/deleted, the error propagates to the decryption of all the blocks from that point on
  - E. an IV is used to randomize the first cyphertext block
  - F. it's resistant to known-plaintext attacks
  - G. random access to blocks (you can decrypt a block independently from the others)

Question 7

- **If you encrypt 50B of plaintext with AES-128-CBC, how long is the ciphertext?**
  - A. 50B
  - B. 64B
  - C. 80B
- **In the above case, let's assume the ciphertext is a secret message to be sent by Alice to Bob. Indicate the size of data transmitted so that Bob can recover the plaintext**
  - A. 50B
  - B. 64B
  - C. 80B

Question 8

- **If you encrypt 50B of plaintext with AES-256-CBC, how long is the ciphertext?**
  - A. 50B
  - B. 64B
  - C. 80B
- **In the above case, let's assume the ciphertext is a secret message to be sent by Alice to Bob. Indicate the size of data transmitted so that Bob can recover the plaintext**
  - A. 50B
  - B. 64B
  - C. 80B
  - D. 96B

Question 9

- **If you encrypt 32B of plaintext with AES-128-CBC, how long is the ciphertext?**
  - A. 32B
  - B. 48B
  - C. 64B
- **If you encrypt 32B of plaintext with AES-128-CTR, how long is the ciphertext?**
  - A. 32B
  - B. 48B
  - C. 64B

Question 10

- **Assume Alice wants to protect her data (1 TB) on disk, but she does not want to increase the space occupied on disk. Moreover, she would like to perform the encryption very fast and to keep her data protected for 10 years. Which algorithm should she use?**
  - A. AES-128-CBC
  - B. AES-128-ECB
  - C. AES-256-CTS-CBC
  - D. 3DES-168-CTS-CBC
  - E. AES-512-CTS-CBC

Question 11

- **Assume Alice wants to protect her data (1 TB) on disk, she has more space, but she would like to perform the encryption very fast. Which algorithm should she use?**
  - A. AES-128-CBC
  - B. AES-128-ECB
  - C. AES-256-CTR
  - D. 3DES-168-CTR
  - E. AES-512-CTS-CBC
  - F. Chacha20-256
  - G. Chacha20-512
  - E. RC4-128

Question 12

- **Which of the following statements are true for the CTR mode:**
  - A. allows parallel encryption of plaintext
  - B. allows parallel decryption of plaintext
  - C. allows random access to groups
  - D. if a ciphertext block is modified, then (only) that group is erroneously decrypted (but not the successive ones)
  - E. it is difficult to perform cryptanalysis because identical plaintext groups encrypt differently
  - F. it's possible to rearrange/swap cyphertext groups
  - G. if a ciphertext group is deleted, all successive cyphertext groups will be decrypted erroneously

Exercises
(symmetric crypto)

Exercise 1

- **Alice wants to send a confidential message P to Bob … and**
  - Alice and Bob have 64 bit platforms
  - P is large, e.g. 10 GB
  - P must be protected for 2 months
- **Alice and Bob have agreed OOB about an algorithm (AES-128-CBC) and a key (K)**
- **write the formulas and the steps**

Questions
(Part II)

Question 13

- **Which of the following algorithm is based on the fact that it is hard to factor large numbers into two prime numbers?**
  - A. ECC
  - B. RSA
  - C. Diffie-Hellman
  - D. DES

Question 14

- **Assume Alice wants to communicate to Bob her public key. She decides to sends the key over an unprotected channel, because the public key is public. Assume Eve can control the communication channel between Alice and Bob. What kind of security attacks could do Eve to damage the secure communication between Alice and Bob?**
  - A. replay attack – Eve sends the public key of Alice 10 times
  - B. sniffing attack – Eve reads the public key of Alice
  - C. man in the middle – Eve modifies the public key of Alice by changing some bits
  - D. man in the middle – Eve replaces the public key of Alice with her own
  - E. filtering – Eve deletes the public key of Alice

Question 15

- **A sender (Alice) wants to send a digitally signed message to a receiver (Bob). Which key is used to create a digital signature?**
  - A. The receiver's private key
  - B. The sender's public key
  - C. The sender's private key
  - D. The receiver's public key

Question 16

- **What is the advantage of RSA over DSA?**
  - A. It can provide digital signature and encryption functionality.
  - B. It uses fewer resources and encrypts faster because it uses symmetric keys.
  - C. It is a block cipher rather than a stream cipher.
  - D. It employs a one-time encryption pad.

Question 17

- **Which of the following best describes a digital signature?**
  - A. A method of transferring a handwritten signature to an electronic document
  - B. A method to encrypt confidential information
  - C. A method to provide an electronic signature and encryption
  - D. A method to let the receiver of the message verify the source (data origin) and integrity of a message

Question 18

- **Diffie-Hellman is a:**
  - A. symmetric algorithm
  - B. asymmetric algorithm
  - C. hash algorithm
  - D. keyed-digest algorithm
- **… that is frequently used for:**
  - A. creating digital signatures
  - B. agreeing on a secret key
  - C. creating an HMAC

Question 19

- **Alice wants to send a secret key K to Bob by using asymmetric cryptography. Which operation must Alice do?**
  - A. encrypt the key K with the public key of Bob, by using RSA
  - B. encrypt the key K with the public key of Bob, by using DSA
  - C. encrypt the key K with her own public key, by using RSA
  - D. encrypt the key K with the private key of Bob, by using DSA