Information Systems Security: exercises on cryptographic techniques for cybersecurity (part II)

Diana Berbecaru

< diana.berbecaru @ polito.it >

Politecnico di Torino

Dip. Automatica e Informatica

AA 2023-2024

Outline

- **questions/problems (multiple-choice)**
  - part 1: message integrity and authentication
  - part 2: X.509v3 certificates, CRL, OCSP, digital signatures
- **exercises**
  - message integrity & asymmetric crypto
- **questions/problems (multiple-choice)**
  - part 3: authentication

Questions
(Part I: message integrity and authentication)

Question 1

- **Which of the following ones are properties or characteristics of a one-way function?**
  - A. converts an arbitrary length message into a fixed-length value (the digest)
  - B. given the digest value h(m), it should be computationally infeasible to find the corresponding message m
  - C. it should be impossible or infrequent to derive the same digest from two different messages
  - D. converts a fixed-length message to an arbitrary length value

Question 2

- **Assume Alice sends to Bob a plain message m along with its digest md=h(m) over an insecure channel. Assume Eve is an active attacker controlling the channel between Alice and Bob (i.e. can read, delete, modify, inject data). Bob receives both the message and the digest. What would tell Bob that the message has been modified?**
  - A. the public key has been altered
  - B. the message digest has been altered
  - C. the message digest computed by Bob is different from the one sent by Alice
  - D. the message extracted by Bob from the digest – i.e. $mBob=h^{-1}(md)$ – is different from the message received m
  - E. none of the above

Problem 1

- Alice wants to protect for integrity one file F on her disk (unprotected). She performs these steps:
  1. she calculates a digest of the file, D = h(F)
  2. she copies D on a secure storage (e.g. a USB pen) where she also keeps other sensitive data (e.g. her RSA key-pair)

  After one year, Alice wants to check if F has been illegally modified, so she takes the file F from disk and recalculates the digest on the file, D' = h(F)

Problem 1 - question

- **What would indicate to Alice that F has been modified?**
  - A. the file F has a different creation time
  - B. the private key has been altered
  - C. the message digest D stored in the secure storage is different from the message digest D' recalculated on F
  - D. the message digest D stored in the secure storage is the same as the message digest D' recalculated on F
  - E. none of the above

Question 3

- **If different messages generate the same hash value, how is this called?**
  - A. secure hashing
  - B. collision
  - C. MAC generation
  - D. HMAC generation

Question 4

- **Given a message m1, after 100,000 random attempts Alice finds a message m2 that generates the same hash value when calculated with the algorithm H. Is H a secure hash algorithm?**
  - A. yes
  - B. no
  - C. it depends on the length of the output generated by H
  - D. it depends on the key used in the computation

Question 5

- **HMAC is an algorithm that allows:**
  - A. to combine a message with a symmetric key to provide data authentication and integrity
  - B. to combine a message with an asymmetric private key to provide data authentication and integrity
  - C. to combine a message with an asymmetric public key to provide data authentication and integrity
  - D. to combine a message with a symmetric key to provide data authentication, integrity, and non-repudiation
  - E. to combine a message with an asymmetric private key to provide data authentication, integrity, and non-repudiation

Question 6

- **Which of the following best describes the difference between HMAC and CBC-MAC?**
  - A. HMAC creates a message digest and is used for integrity; CBC-MAC is used to encrypt blocks of data for confidentiality
  - B. HMAC uses a symmetric key and a hash algorithm; CBC-MAC uses the first encrypted block as a checksum
  - C. HMAC and CBC-MAC provide integrity and data authentication; HMAC uses a hash function, while CBC-MAC uses a block encryption algorithm
  - D. HMAC encrypts a message with a symmetric key and then puts the results through a hash algorithm; CBC-MAC encrypts the whole message

Question 7

Alice wants to protect some messages m1, m2, … mN for data authentication and integrity. She constructs for each message a MAC in the following manner:

for (i=1; i<=N; i++) mac(i) = HMAC-SHA256(i, m_i);

She sends each message m_i and the corresponding mac(i) to Bob over an unprotected channel.

Is data authentication and integrity achieved for all messages m_i? (justify your answer)

- A. yes
- B. no

Question 8

- **Alice wants to send Bob a plaintext P protected for confidentiality, authentication, and integrity**
- **Alice and Bobs share two symmetric keys K1 and K2**
- **Alice and Bob agreed on two algorithms, A1 (for MAC) and A2 (for symmetric encryption)**
  - which operations should Alice perform on P and what data should she transmit to Bob so that he can recover the plaintext and verify its integrity and authenticity?
  - explain the advantages and disadvantages of your solution

Question 10

- **Authenticated Encryption provides:**
  - A. confidentiality and authentication/integrity in one step with two different keys
  - B. confidentiality and authentication/integrity in one step with one key
  - C. confidentiality and authentication/integrity in two steps with one key

Questions
(Part II: X.509v3 certificates, CRL, OCSP, digital signatures)

Question 1

- **Which of the following best describes a Certification Authority?**
  - A. an organization that issues private keys and the corresponding algorithms
  - B. an organization that certifies encryption algorithms
  - C. an organization that certifies encryption keys
  - D. an organization that issues public-key certificates to entities

Question 3

- **Assume a CA issues an X.509v3 certificate to Alice. Which of the following values are included in the certificate issued to Alice? Select all that apply.**
  - A. Alice's public key
  - B. Alice's private key
  - C. A signature on Alice's X.509v3 certificate, calculated with the CA's private key
  - D. A signature of the Alice's X.509v3 certificate, calculated with the CA's public key
  - E. An indication of the owner of the certificate, such as the Alice's name or e-mail address
  - F. A time period, indicating the lifetime of the certificate
  - G. An indication of the issuer of the certificate, such as the CA's name

Question 4

- **Why would a Certification Authority revoke a certificate?**
  - A. if the subject's public key has been compromised
  - B. if the subject's private key has been compromised
  - C. if the subject sent the certificate over an unprotected channel
  - D. none of the above

Question 5

- **Which of the following statements about CRL and OCSP are correct?**
  - A. CRL is a list of revoked certificates issued by a CA
  - B. CRL is a list of revoked certificates issued by a root CA
  - C. OCSP is a protocol to query a server about the validity of a single specific certificate at a specified time
  - D. OCSP is a protocol to query a server about the validity of a single specific certificate at the current time

Question 6

- **Alice sends a digitally signed message to Bob and attaches her X.509v3 certificate (and a certificate chain up to a trusted root CA). Which steps must Bob perform to verify the signature on the message? (you can select multiple responses from the ones below)**
  - A. verify the signature on the message by using the certificate of Alice
  - B. verify that the certificate of Alice is authentic by constructing the chain up to a trusted root and verifying the signatures on each certificate in the chain
  - C. verify that each certificate in the chain (except the one of the trusted root) has not been revoked
  - D. do not check the trusted root CA certificate that Alice sent him because he should have it already configured it as trusted

Exercises
(integrity & asymmetric crypto)

Exercise 1a

- **Alice wants to send to Bob a message P protected for integrity and (data) authentication**
  - Alice and Bob share a symmetric key K
  - Alice and Bob agreed about using HMAC-SHA1
- **what information should Alice send to Bob? (write the corresponding formulas)**

Exercise 1b

- **Alice wants to send to Bob a message P protected for integrity and (data) authentication**
  - Alice and Bob share a symmetric key K
  - Alice and Bob agreed about using HMAC
- **what information should Alice send to Bob? (write the corresponding formulas)**

Exercise 2

- **Alice wants to send a confidential message P to Bob … and**
  - P is large, e.g. 10 GB
  - P must be protected for 4 months
- **Alice and Bob have agreed about an asymmetric encryption algorithm (RSA), and a symmetric one (AES-128-CBC) and exchanged OOB their respective public keys**
- **write the formulas and the steps**

Exercise 3

- **Alice wants to send to Bob a digitally signed message P**
- **assumptions:**
  - Alice has an RSA key pair (Alice.SK, Alice.PK)
  - Bob knows Alice.PK (may be it was exchanged OOB)
- **write down the formulas**

Problem 1

- **Two companies in business wish to protect their messages (exchanged via an unprotected TCP/IP network) by providing confidentiality, integrity, and data authentication. Assuming that the companies do not have access to any secure channel or data format but share a password pwd (10 alphanumeric characters long) and can use only basic symmetric encryption, hash algorithms, and auxiliary mathematical functions (but not asymmetric encryption), suggest a possible solution for protecting a message M and write the formula to generate the protected message P.**

Questions
(Part III : Authentication)

Question 1

- **Which of the following statements correctly describes reusable passwords as authentication factor?**
  - A. they are the least expensive and most secure
  - B. they are the most expensive and least secure
  - C. they are the least expensive and least secure
  - D. they are the most expensive and most secure

Question 2

- **Which of the following factors provides stronger authentication?**
  - A. what a person knows
  - B. what a person is
  - C. what a person has

Question 3

- **How is a challenge/response protocol used with an authentication-token (device)?**
  - A. this protocol is not used; cryptography is used
  - B. an authentication service generates a challenge, then the authentication token generates a response based on the challenge
  - C. the token challenges the user for a username and password
  - D. the token challenges the user's password against a database of stored credentials

Question 4

- **What is a dictionary attack?**
  - A. the attacker pre-computes a list of hashes of many "words"; the hashes are then compared with a hashed password (sniffed from the communication channel or leaked from a server)
  - B. the attacker pre-computes several hashes (for several iterations) starting from a word in the Dictionary; the hashes are then compared with a hashed password (sniffed from the communication channel or leaked from a server)
  - C. the attacker uses a Dictionary of common words (e.g. English language dictionary) to pre-compute a big list of their hashes; the hashes are then compared with a hashed password (sniffed from the communication channel (or leaked from a server)

Question 5

- **A salt is used to protect from dictionary attack. A salt is ..**
  - A. a secret number
  - B. a random number, unpredictable
  - C. a number that must be known only by the user to generate a more secure password

Question 6

- **The advantages of static passwords are (you can choose more than one option):**
  - A. are simple, "free", and require no extra device to carry
  - B. are immune to sniffing
  - C. are immune to replay attacks
  - D. require no trust in a third party (in contrast, public key certificates require trust in the CA)
  - E. are immune to MITM attacks

Question 7

- **The advantages of OTPs are (you can choose more than one option):**
  - A. are simple, "free", and require no extra device to carry
  - B. sniffing attacks are not efficient
  - C. are immune to replay attacks
  - D. require no trust in a third party (in contrast, public key certificates require trust in the CA)
  - E. are immune to MITM attacks

Question 8

- **A claimant must authenticate to a Verifier by using a symmetric CRA protocol. The advantages in this case are (you can choose multiple options):**
  - A. the Verifier must not store sensitive keys
  - B. sniffing attacks are not efficient
  - C. replay attacks cannot be performed
  - D. require no trust in a third party (in contrast, public key certificates require trust in the CA) or OOB exchange of public keys
  - E. is fast
  - F. is immune to involuntary signing or to relay attacks (does not require Verifier authentication)

Question 9

- **A claimant must authenticate to a Verifier by using an asymmetric CRA protocol. The advantages in this case are (you can choose multiple options):**
  - A. the Verifier must not store sensitive keys
  - B. sniffing attacks are not efficient
  - C. replay attacks cannot be performed
  - D. require no trust in a third party (in contrast, public key certificates require trust in the CA) or OOB exchange of public keys
  - E. is fast
  - F. is immune to involuntary signing or relay attacks (does not require Verifier authentication)