Practice Questions + Answers for the Midterm (ECS655U-ECS755P)

Dr Na Yao, Dr Arman Khouzani

Queen Mary University of London

February, 2018

1. List three security services. [3 marks]

Solution: Confidentiality, Data integrity, Data origin authentication, Non-repudiation, Entity authentication (1 mark for each service, total 3 marks)

2. Consider the scenario of an e-commerce website like Amazon where customers can register an account and purchase items online with secure transactions. Give examples of the security services the system should provide in terms of confidentiality, and data integrity. [4 marks]

Solution: The website must keep the account information confidential, both in the server and during the transaction [2 marks]. It must protect the integrity of account information/purchase information, that is, no unauthorised alteration to these information[2 marks]

3. Define the terms: plaintext, ciphertext, encryption algorithm. [3 marks]

Solution: The plaintext is the raw data to be protected during transmission from sender to receiver. [1 mark] The ciphertext is the scrambled version of the plaintext that results from applying the encryption algorithm (and the encryption key) to the plaintext. [1 mark] The encryption algorithm is the set of rules that determines, for any given plaintext and encryption key, a ciphertext. [1 mark]

4. What’s the difference between Symmetric and Public-key cryptosystem? [4 marks]

Solution: In symmetric cryptosystems, the encryption key and the decryption key are essentially the same. [2 marks] In public-key cryptosystems, the encryption key and the decryption key are fundamentally different. [2 marks]

5. Caesar Cipher is a historical cryptosystem where each letter of the English alphabet is encrypted by ‘shifting’ the alphabet a secret number of positions. What’s the keyspace of Caesar Cipher? Why? [4 marks]

Solution: there are 26 possible different shifts, each of which corresponds to a possible key, so the keyspace has size 26. [4 marks]

6. What’s perfect secrecy? Give an example of a cryptosystem that achieves perfect secrecy in theory. [5 marks]

Solution: We say a cryptosystem has *perfect secrecy* if, after seeing the ciphertext, an interceptor *gets no extra information about the plaintext other than what was known before the ciphertext was observed*. One-time pad can achieve perfect secrecy in theory.

7. Explain stream cipher. What’s the error propagation of stream cipher that uses XOR function, if there is 1-bit transmission error in the ciphertext? [5 marks]

Solution: In *Stream ciphers*, the plaintext is processed one bit at a time. Since stream ciphers encrypt the plaintext bit by bit, a 1-bit transmission error will only result in a 1-bit error in the plaintext.

8. AES is a block cipher. Explain what is a block cipher. What's the error propagation of a block cipher? [5 marks]

Solution: In *Block ciphers*, the plaintext is processed in *blocks* (groups) of bits at a time. A 1-bit transmission error only changes one bit of a ciphertext block, but the result of decrypting this erroneous ciphertext block will be a plaintext block with, on average, half of its bits incorrect, due to the diffusion property.

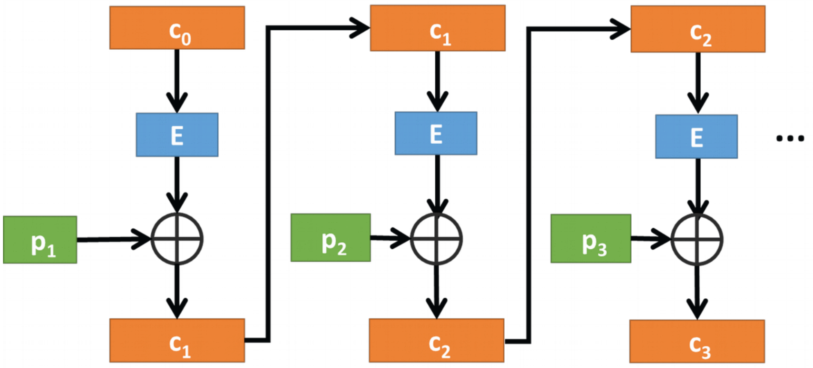
9. Discuss the differences between Stream ciphers and Block ciphers, in terms of the way plaintexts is processed and error propagation. [5 marks]

Solution: In *Stream ciphers*, the plaintext is processed one bit at a time. Since stream ciphers encrypt the plaintext bit by bit, a 1-bit transmission error will only result in a 1-bit error in the plaintext. In *Block ciphers*, the plaintext is processed in *blocks* (groups) of bits at a time. A 1-bit transmission error only changes one bit of a ciphertext block, but the result of decrypting this erroneous ciphertext block will be a plaintext block with, on average, half of its bits incorrect, due to the diffusion property.

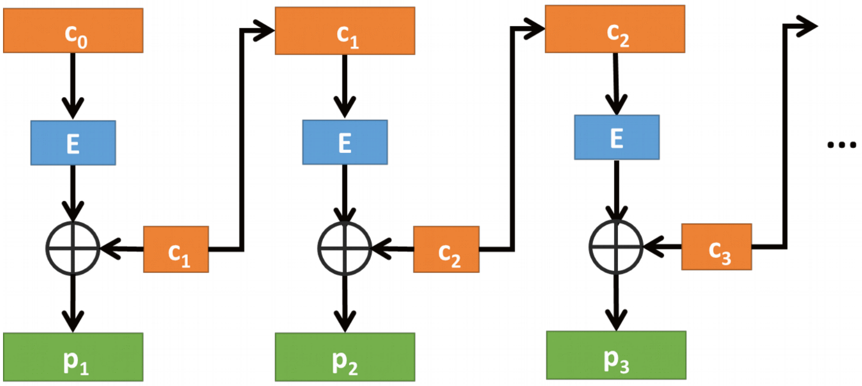
10. Block ciphers are often used in different modes of operations, and Electronic Code Book(ECB) mode is a basic mode of operation. Explain how ECB works (you can use a diagram to help). [5 marks]

Solution: In ECB mode, we take the first block of plaintext and encrypt it with the key to produce the first block of ciphertext. We then take the second block of plaintext and encrypt it with the key to produce the second block of ciphertext, etc.

11. The diagram below gives the encryption for Cipher FeedBack (CFB) mode. Draw a diagram for the decryption of CFB mode and label each element clearly.



Solution:



12. What’s the error propagation for Cipher Block Chaining (CBC) mode if 1-bit transmission error happens for ciphertexts? Why? [5 marks]

Solution: If 1-bit transmission error happens for ciphertexts, in CBC mode, the block where transmission error happens will give wrong plaintext block, as well as the next plaintext block. This is because CBC mode a ciphertext block depends on current plaintext and previous ciphertext block.

13. Public-key cryptography uses trapdoor one-way functions. Explain what is a trapdoor one-way function. [5 marks]

Solution: A one-way function is a function that is easy to compute in one way, but hard to reverse. i.e. given x it’s easy to compute f(x), but given f(x) it’s hard to compute x. A trapdoor one-way function is a one-way function f , together with a secret y, such that, given f(x) and y, it is easy to compute x.

14. Briefly explain the security of RSA algorithm, in terms of 1. Decrypting a Ciphertext Without Knowledge of the Private Key and 2. Determining the Private Key Directly from the Public Key. [5 marks]

Solution: 1. $c = m^e \bmod n$

Computing m from c, e, and n is believed (but never proved) to be a hard problem, called “the RSA problem”, and thus the encryption function of RSA is considered a one-way function.

2. To determine a private key *d* from a public key (*n*, *e*), an attacker need to:

- Factor *n=pq*, into its prime factors *p* and *q* are; and
- Run the Extended Euclidean Algorithm to determine *d* from *p*, *q*, and *e*.

Factoring the product of two large prime numbers is believed to be a hard problem, so it’s very hard to determine private key d from public key.

15. Briefly explain the security of ElGammal algorithm, in terms of 1. Decrypting a Ciphertext Without Knowledge of the Private Key and 2. Determining the Private Key Directly from the Public Key. [5 marks]

Solution:

- Difficulty of decryption without private key == Difficulty of discrete logarithm, i.e., solving $\mathbf{g^k \bmod p}$ *for k* .
- Difficulty of deriving private key from public key == Difficulty of discrete logarithm, i.e., solving $\mathbf{g^x \bmod p}$ *for x*.

16. What is a cryptographic hash function? Explain the three security properties of a cryptographic hash function. [5 marks]

Solution: A cryptographic *hash function* is a mathematical function that takes variable length input and generate fixed length output, and hash functions are used in cryptographic systems to achieve data integrity. Security property 1: for a hash function *h*, given an output (hash) value *z*, it should be difficult to find any input value *x* which hashes to *z*. (*preimage-resistant*) Security property 2: given an input and its hash, it should be hard to find a *different* input with the *same* hash. (*second-preimage-resistant*) Security property 3: it should be hard to find two different inputs (of any length) that, when fed into the hash function, result in the same hash being computed. (*collision resistance*)

17 What is Message Authentication Code (MAC)? Explain how MAC can be used to provide data origin authentication. [5 marks]

Solution: MAC is a cryptographic checksum which is sent along with a message in order to provide an assurance of data origin authentication. The sender and receiver share a symmetric key *K*. The MAC takes as input the message and the key *K*. The sender transmits the message accompanied by the MAC. Upon receipt of the message and the MAC, the receiver inputs the received message and the key into the MAC algorithm and recomputes the MAC. The receiver then checks whether this freshly recomputed MAC matches the MAC sent by the sender. If they do match, then the receiver accepts the message and regards data origin authentication as having been provided.

18 Alice would like to send a message to Bob and she wants to ensure the message is confidential and Bob is certain that the message is from Alice. Explain how Alice can achieve this using encryption and MAC. [5 marks]

Solution: Alice can generate a MAC checksum then encrypt the message and MAC, and send the ciphertext to Bob. (Alternatively Alice can encrypt the message, then generate a MAC on the ciphertext, then send both ciphertext and MAC to Bob) When Bob receives the message, he can decrypt the message, then calculate a new MAC, and comparing the fresh MAC to the MAC sent from Alice.

19. Briefly explain the general requirements for a digital signature scheme. [5 marks]

Solution: a *digital signature scheme* should provide:

- **Data origin authentication of the signer**. A digital signature validates the underlying data in the sense that assurance is provided about the integrity of the data and the identity of the signer.
- **Non-repudiation**. A digital signature can be stored by anyone who receives it as evidence. This evidence could later be presented to a third party who could use the evidence to resolve any dispute relating to the contents and/or origin of the underlying data.

20. Briefly explain the signing process using RSA digital signature scheme. [5 marks]

Solution: 1. The signer starts by hashing the data being signed. 2. The signer now signs the hashed data. This process simply involves 'encrypting' the hashed data using RSA as the encryption algorithm and the signer's signature key as the 'encryption' key. 3. The signer sends to the verifier two pieces of information: a the data itself; and the digital signature.

21. Explain why hash functions are applied to the message first in RSA digital signature scheme. [5 marks]

Solution: The reasons are 1. Hash function produce a small digest of the data being signed, and it's more efficient to sign the digest than the entire message using RSA. (It is very slow to encrypt large amount of data using RSA) 2. Using hash function will prevent modification attack, and 3. Prevent existential forgeries where attacker can generate a signature and "decrypt" the signature with verification key to produce a piece of message.

22. What is entity authentication? [5 marks]

Solution: Entity authentication is the assurance a given entity is involved and currently active in a communication session. This means entity authentication really involves assurance of both:

- **Identity**. The identity of the entity who is making a claim to be authenticated.
- **Freshness**. The claimed entity is ‘alive’ and involved in the current session.

23. For entity authentication, it is important to ensure the “freshness” of a communication entity. List three freshness mechanism and briefly explain each of them. [5 marks]

Solution: 1. Clock-based freshness mechanism. A *clock-based* freshness mechanism is a process which relies on the generation of some data that identifies the time the data was created. This is sometimes referred to as a *timestamp*. 2. Sequence numbers freshness mechanism. In applications where clock-based mechanisms are not appropriate, an alternative mechanism is to use *logical* time. Logical time maintains a notion of the order in which messages or sessions occur and is normally instantiated by a *counter* or *sequence number*. 3. Nonce-based mechanisms. *Nonces* (literally, ‘numbers used only once’), which are randomly generated numbers for one-off use.

24. For dynamic password schemes, explain how dynamic password schemes are more advantageous than passwords, in terms of vulnerability and repeatability ? [5 marks]

Solution: 1. Dynamic password schemes limit the exposure of the password, thus reducing vulnerability; and 2. Dynamic password schemes use the password to generate dynamic data which changes on each authentication attempt, thus preventing repeatability.

25. What is a cryptographic protocol? List the main components of a cryptographic protocol.[5 marks]

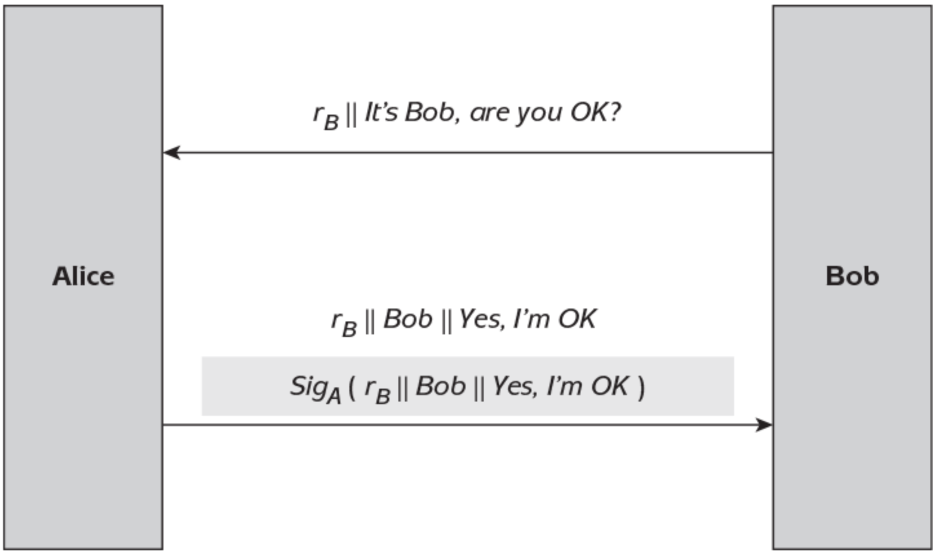
Solution: A *cryptographic protocol* is a specification of all the events which need to take place in order to achieve some required security goals. In particular, a cryptographic protocol needs to specify: The protocol assumptions, The protocol flow, The protocol messages, The protocol actions.

26. List three typical goals of an authentication and key establishment (AKE) protocol, and briefly explain each of them. [5 marks]

Solution: the typical goals include:

- **Mutual entity authentication**. Alice and Bob are able to verify each other’s identity to make sure they know with whom they are establishing a key.
- **Mutual data origin authentication**. Alice and Bob can be certain that information being exchanged originates with the other party and not an attacker.
- **Mutual key establishment**. Alice and Bob establish a common symmetric key.
- **Key confidentiality**. The established key should at no time be accessible to any party other than Alice and Bob.
- **Key freshness**. Alice and Bob should be happy that (with high probability) the established key is not one which has been used before.
- **Mutual key confirmation**. Alice and Bob should have some evidence that they both end up with the same key.
- **Unbiased key control**. Alice and Bob should be satisfied that neither party can unduly influence the generation of the established key

27. Below is a diagram for a cryptographic protocol between Alice and Bob. Does the protocol provide Data origin authentication of Alice's reply? Explain your answer. [5 marks]


Alice
Bob
r_B || It's Bob, are you OK?
r_B || Bob || Yes, I'm OK
Sig_A (r_B || Bob || Yes, I'm OK)

Where rB is A nonce generated by Bob, || denotes Concatenation, SigA(data) is a digital signature on data computed by Alice, and Bob is an identifier for Bob (perhaps his name).

Solution: We assume that Alice has been issued with a signature key, and Bob has access to a verification key corresponding to Alice's signature key. The only entity who can compute the correct digital signature on the reply text is Alice. Thus, given that her digital signature is verified, the received digital signature must have been computed by Alice. Thus, Bob indeed has assurance that the reply was generated by Alice.

28. In key management, explain the terms *key generation* and *key establishment*. [5 marks]

Solution: *Key generation* concerns the creation of keys. *Key establishment* is the process of making sure keys reach the end points where they will be used.

29. A *public-key certificate* is data binding a public key to data relating to the assurance of purpose of this public key. List the four main contents of a public-key certificate and briefly explain each of them.[5 marks]

Solution: **Name of owner**. The name of the owner of the public key. **Public-key value**. The public key itself. **Validity time period**. This identifies the date and time from which the public key is valid and, more importantly, the date and time of its expiry. **Signature**. The creator of the public-key certificate digitally signs all the data that forms the public-key certificate, including the name of owner, public-key value, and validity time period.

30. Briefly explain Diffie–Hellman key agreement and its purpose. [5 marks]

Solution: The purpose of the algorithm is to enable two users to securely exchange a key that can then be used for subsequent encryption of messages. The algorithm itself is limited to the exchange of secret values. The Diffie-Hellman algorithm depends for its effectiveness on the difficulty of computing discrete logarithms.