IK2206 – Internet Security and Privacy

Exam Questions

This document contains questions of previous IK2206 exams as they were published by the course administration. The exam consists of two parts, A and B. There are multiple choice questions in part A whereas part B poses open text questions. For some of the given multiple choice questions in part A below only the correct answer (and a comment) is listed. To get part B corrected, part A has to be passed with a minimum number of points (~75% correct).

Part A

A:1 1p. Can secret key cryptography be used for digital signatures?

No, the verifier needs access to the secret key.

Comment: Section 2.5: If the verifier has the key he could have created the signature. If the key is kept secret, no one can verify the signature.

A:2 1p. Which of the following would be unsuitable to use as a nonce?

A public key.

Comment: Section 11.5: A public key is, most likely, used more than once.

A:3 1p. Public key cryptography algorithms have a number of important properties. Which of the following statements about these algorithms is false?

The property $K^{-}(K^{+}(m)) = m = K^{+}(K^{-}(m))$ is very important in the Diffie-Hellman algorithm.

Comment: $K^{-}(K^{+}(m)) = m = K^{+}(K^{-}(m))$ *is true for RSA, but not for Diffie-Hellman*

A:4 1p. In RSA, given the public key <n,e> and the private key <n,d> where n = pq, the following is true:

one way to find d from <n,e> is to first find p and q.

Comment: Section 6.2: If you answered that n is a prime than think again!

A:5 1p. In Diffie-Hellman, when Alice sends ga mod p to Bob then . . .

g and p are not secrets.

Comment: Section 6.4 : In fact g and p could be part of the standard but then someone would compute ga mod p for all possible a (although that would take some time and space).

A:6 1p. Alice and Bob want to communicate in a secure way using public-key encryption, and therefore agree on the following protocol: Suppose that Alice wants to send a message to Bob. First she computes the hash of the message using a cryptographic hash function. She encrypts the hash with her private key. Then she encrypts the message with Bob's public key. She sends the encrypted hash as well as the encrypted message to Bob. What kind of security can Alice and Bob achieve in this way?

Integrity, confidentiality, and authenticity.

Comment: Integrity, since no one (except Alice) can modify both the message and the hash. Confidentiality, since only Bob can decrypt the message. Authenticity, since the hash can be decrypted with Alice's (certified) public key.

A:7 1p. Alice and Bob want to communicate in a secure way using public key encryption, and therefore agree on the following protocol: Suppose that Alice wants to send a message m to Bob. She uses a cryptographic hash function H to compute the hash of the message, H(m). Using her private key, she encrypts the message together with the hash and gets K^{-}_{Alice} (m,H(m)), which she sends to Bob. What kind of security would Alice and Bob achieve in this way?

Integrity and authenticity.

Comment: Integrity, since no one (except Alice) can modify both the message and the hash. Authenticity, since only Alice could have encrypted the message with her private key. Not confidentiality, since anyone can decrypt the message using Alice's public key.

A:8 **A:4** 1p. Which of the following changes would not increase the crypto-graphic strength of DES?

Increasing the number of permutations in each round.

Comment: Increasing the block size. Permutations do not increase the cryptographic strength of a cipher

A:9 1p. How can a 3DES implementation using EDE (encrypt-decrypt-encrypt) interoperate with single DES encryption?

It will use k1 = k2 = k3.

Comment: If all two resp. three keys in 3DES are equal, then 3DES interoperates with DES.

A:10 1p. Regular DES is considered insecure and is not used in applications with strict demands on security. What is the main problem with regular DES?

The keys are too short.

Comment: The key is so short that a brute-force attack is possible.

A:11 1p. Which statement is true? A stream cipher:

can often be computed faster, and with lower complexity, compared to a block cipher.

Comment: implements a one-time pad and is therefore unbreakable. Section 3.6 and 4.2: We do not have to wait for a block to be filled neither at the sender nor at the receiver.

A:12 1p. What are the names of the two basic transformations in the implementation of a block cipher?

Permutation and substitution.

Comment: Section 3.2

A:13 1p. Cipher Block Chaining (CBC) generates a sequence of ciphertext blocks from a sequence of plaintext block. Which alternative describes most correctly how cipherblocks are computed?

A ciphertext block is computed from the encryption key, the plaintext block, and the preceeding ciphertext block.

Comment: Section 4.2

A:14 1p. Using mod n multiplication as a message digest function is not good since . . .

it is easy to construct a message with a given digest.

Comment: Section 5.1

A:15 1p. Which of the following would not be a generally accepted requirement for a message digest function H?

If there is a message m and a digest d such that H(m) = d, there is no other message n such that m 6= n and H(n) = d.

Comment: Section 5.1 : A message digest is a many-to-one mapping, so collisions are unavoidable.

A:16 1p. Consider a UNIX password database that stores a password digest together with a salt.

The salt introduces randomness in the digests, which makes it more difficult for an attacker to stage an attack by pre-computing digests.

Comment: Section 10.3: The salt is normally stored with a hashed password. When you want to check if a password is valid you need to hash the password with the salt (or have the salt modify the hash algorithm).

A:17 1p. The RSA algorithm is computationally complex, and thus expensive. Which of the following methods is not a good way to reduce the cost of using RSA?

We can use small primes for n.

Comment: Section 6.3

A:18 1p. Assuming we have no previous knowledge,…

neither Diffie-Hellman nor RSA can be used for authentication.

Comment: Section 6.4

A:19 1p. We talk about using biometrics for identification and authentication, but what do we mean when we say ”biometrics”? Which of the following examples is the best definition?

Biometrics are any measurements of unique or semi-unique properties of the body of the person being identified/authenticated.

Comment: Both things like DNA as well as finger prints are examples of biometrics. Indeed, anything you can measure from a person's body, inside (like blood) or outside (like the voice or the ear shape), can work. Things you remember, on the other hand, are not biometrics.

A:20 **A:**11 1p. Lamport's hash is used to . . .

authenticate a client to a server over an insecure channel.

Comment: Section 12.2: The problem is that we have to store a new hash in the server every now and then.

A:21 1p. Assume that Alice wants to authenticate herself to Bob using Kerberos (Bob is a server, in Kerberos terminology). How is the Kerberos Ticket Granting Ticket (TGT) used in this context?

It is used so that the Ticket Granting Server (TGS) need not store the session keys of Alice.

Comment: Section 13

A:22 1p. In a KDC-based system, Alice receives a ticket from the KDC for communication with Bob. In the subsequent communication with Bob, Alice also uses an authenticator. Which of the following statements is not true?

The authenticator is created by the KDC.

Comment: Section 13.4: It can then be decrypted by Bob, and Alice and Bob will share a session key.

A:23 1p. Alice uses Kerberos for authentication in order to get access to a server. The authentication is done through Kerberos, so it includes a Key Distribution Center and a Ticket Granting Server. Alice will receive a ticket from the Ticket Granting Server, and for this purpose the communication between Alice and the Ticket Granting Server is encrypted with a secret key shared between Alice and the Ticket Granting Server. The key shared between Alice and the Ticket Granting Server:

is created by the Key Distribution Center.

Comment: Section 13

A:24 1p. When a certificate is revoked, it means that:

The CA has invalidated the certificate.

Comment: A certificate being revoked does not mean it wasn't correctly issued or valid, only that it isn't valid any longer.

A:25 1p. Recently, it was discovered that RAs of a major CA called Comodo had been compromised, and bogus certificates for several well-known addresses, including login.yahoo.com, login.skype.com and mail.google.com were created by the intruders. Which is the best and most secure response to this breach?

Download and install the Certificate Revocation List from Comodo.

Comment: Tempting as it may be to remove the root certificate for Comodo, doing so will mean that you no longer will be able to authenticate many sites with certificates issued by Comodo, and thus be less secure than even if you did nothing.

A:26 1p. A PKI certificate is . . .

a name and a public key signed using the private key of a certificate authority.

Comment: Section 15.1

A:27 1p. S/MIME uses an oligarcy organization for certificates. An S/MIME certificate is signed by

Any CA (certificate authority) that is recognized as a top-level CA.

Comment: …

A:28 1p. Using IPsec with AH in transport mode will . . .

authenticate the payload and IP header.

Comment: Section 17.1

A:29 1p. Using IPsec with AH the following IP header fields are treated as mutable:

fragmentation offset and header checksum

Comment: Section 17.3

A:30 1p. Which of the following statements about IPsec security associations (SA) is true?

An SA is a one-way sender-recipient relationship.

Comment:

A:31 1p. Authentication in IKE is always implemented using . . .

a negotiated protocol.

Comment:

A:32 1p. Which of the following statements about firewalls is correct?

Packet filtering firewalls can block or allow packets based on data both in packets headers and in the packet payload.

Comment: Section 23

A:33 1p. Which of the following statements about firewalls is false?

UDP traffic cannot be managed by an application level gateway.

Comment: Section 23

A:34 1p. Web cookies can be security issues because they could:

not be properly protected by the client browser.

Comment: Bugs in web browsers is a common cause of cookie security problems.

A:35 1p. What statement about the initial SSL/TLS handshake is incorrect?

The client sends its public-key certificate to the server.

Comment: Section 19.4. This answer is somewhat wrong. In SSL/TLS the server usually does not authenticate the client – only the client makes sure it is talking to the right server. Consider e-commerce solutions: How much sense would it make for a web shop or an e-banking system to check what kind of internet clients they are communicating with?! There are, of course, situations where the client also has to reveal his identity to the server. In this case, each client has to have a valid public key certificate.

A:36 1p. Alice and Bob use SSL/TLS for secret communication. Which of the following statements is true?

Session integrity is achieved by including nonces in the communication.

Comment: Section 18.4

A:37 1p. In SSL/TLS the version rollback attack is avoided by

including the version number in the master secret exchange.

Comment:

A:38 1p. Bob receives an authenticated email from Alice through PGP. What key does Bob use to verify the authenticity of the email?

Alice's public key.

Comment: Section 18.4

A:39 1p. With PGP mail (Pretty Good Privacy), the trust model:

is based on a trust relationship among the users.

Comment: Section 18.4

A:40 1p. Alice sends an encrypted, integrity-protected and authenticated email to Bob using PGP. In order to read and verify the email, Bob will be using three different keys: Alice's public key, Bob's private key, and a temporary, shared session key. In what order will Bob use those keys for decryption?

Bob's private key, session key, Alice's public key.

Comment: Section 18.4. First Bob's private key to decrypt the session key, then the session key to decrypt the message and the digest, and finally Alice's public key to decrypt the message digest to verify integrity/authenticity.

Part B

B:1 2p. In a PKI system, there may be a need to revoke certificates. Explain why certificate revocation may be necessary. Describe two different ways of revoking certificates. Why is it not needed in a KDC system?

Section 15.4. At any time during the validity period, the certificate authority can revoke a certificate. This can occur for many reasons, such as a compromise of the private key of the certificate.

When this occurs, any chains that descend from the revoked certificate are also invalid, and are not trusted during authentication procedures. To find out which certificates are revoked, each issuer publishes a time- and date-stamped certificate revocation list (CRL). The list can be checked using either online revocation or offline revocation. We talk about online revocation if every certificate is validated at the time of the request. When offline revocation is used, the peers usually download CRLs locally from time to time. Offline revocation is much faster but bears the risk of outdated CRL entries. Thus, online revocation is potentially more secure.

A Key Distribution Center (KDC) is not based on public key cryptography; hence, no certificates are used. KDC uses symmetric keys to encrypt communication channels – a completely different approach to solve the same problem…

http://msdn.microsoft.com/en-us/library/ms731899.aspx

B:2 3p. Assume that IPsec ESP is used both for confidentiality and integrity. Illustrate ESP encapsulation of an IP packet containing a TCP segment, both in transport mode and tunnel mode. Show what parts of the packet that are encrypted and authenticated respectively. Your illustrations should include IP header(s), IPsec ESP header/trailer, and the TCP segment, but not any individual header fields.

In transport mode: TCP segment+ESP trailer are encrypted. ESP header+TCP segment+ESP trailer are authenticated. Original IP header remains unchanged in the front of the packet and ESP authentication info comes ends the packet.

New IP Header	ESP Header	Original IP Header	IP Payload	ESP Trailer	ESP Auth.
		Encrypted			
	Authenticated				

In tunnel mode: Original IP header+TCP segment+ESP trailer are encrypted. ESP header+original IP header+TCP segment+ESP trailer are authenticated. A new IP header (tunnel header) is placed in the front of the packet and ESP authentication info ends the packet. See lecture slides from IPsec lecture.

IP Header	ESP Header	IP Payload	ESP Trailer	ESP Auth.
		Encrypted		
	Authenticated			

B:3 3p. Security protocols can be located at different parts of a system, and at differen protocol levels. There are three main methods: at the IP level, between transport protocol and application (TLS/SSL), and integrated into the application. Discuss the advantages and disadvantages of these. For each method, give an example of a situation where the method would be a good choice, and give an example of a situation where the method would not be suitable. Finally, give two examples of applications where security is integrated into the application-level protocol.

IP-level security is suitable when all communication needs to be secure, but requires operating system control (and possible also infrastructure level), so it would not be suitable if you do not have access to those. TLS/SSL is useful if you want to secure a specific application, but in many cases it requires modifications of the application, and does not give system-wide security. Application-level security is useful if you need to tailor the security specifically for the requirements of a specification, but is less useful if you want system-wide security. Examples of application-level security protocols include S/MIME, PGP, SSH and Kerberos.

B:4 4p. Several countries are introducing passports with a built in RFID chip. The chip is passive but will reply when read by a radio scanner. The chip that will be used in passports can typically hold a small amount of data, most probably information such as name, date of birth, photo, biometric data, etc. The idea is that a customs officer can quickly get all the information he/she needs to identify you. There are several problems that must be solved. The first is, how do we know that the information stored on the chip is correct? If I can program a chip, I could claim to be Batman. How would you design a system so that a customs officer, in a faraway country with no network connections, could validate the information?

Another problem is, if anyone can scan your passport they would also know all your personal information. One proposed solution is to print a key, using a bar code, inside the passport. Only the one who can see the bar code will then be able to interpret the information on the chip. How would this work? What encryption technique could be used? Assuming that the chip is very simple and replies with the same data every time it is probed, what threats to privacy do we have even if we cannot interpret the reply?

The first problem is best solved by public key encryption. A message digest of the data is signed using the private key of the passport authority. The public keys of all authorities could be distributed off-line to all customs offices. One would probably use certificates with a time limit thus setting time limit on the passports.

The second problem one could use a simple block cipher in a proper mode of operation. The printed bar code is the secret key used to do the encryption and can thus be used for decryption. It’s of course important that all passports have unique keys.

The third problem is of course that we can track a person once we have his/her unique reply. Even if we cannot interpret the data we know that the person has entered the room, building or city (if we have scanners at all roads). We might also be able to detect how many persons holding passports we have in room. If different countries used different systems we might even know the nationalities.

B:5 3p. The web of trust or anarchy model is an alternative to hierarchical models of building trust.

Explain how the model works, and what trust anchors exist, if any. Are there any specific problems or issues that you must consider as a user of this model?

Need to make observation that you are the ultimate trust anchor in this model. Most of the issues derive from this.

B:6 3p. Suppose there is an error during a transfer of data encrypted in CBC (cipher block chaining) mode. It is single error, so only one ciphertext block is corrupted. What plaintext blocks are affected by the error? Explain!

Suppose the error is in ciphertext block Ci. The corresponding plaintext block Pi will be affected, since Pi is computed from Ci−1 and Ci. Also Pi+1 is affected, since it is computed from Ci and Ci+1

B:7 4p. A large city will soon introduce a toll system where cars passing in and out from the city will have to pay a fee. The system is very advanced and is built using cameras, lasers and radio transponders. Cars will have a transponder with a built-in radio chip that will reply with its identity when requested by a radio scanner. To create an open market for transponders yet protecting the privacy of the public, a KTH student was asked to design an encryption scheme. The presented solution works as follows: The road toll operators generate an RSA public and private key of 1024 bits. The public key is made public and can be used by manufacturers of transponders. When a transponder is questioned it will reply with its registration number encrypted with the public key (for example {”DKP002”}$_{\text{Toll}}$, where Toll is the public key of the operator. Clearly the KTH student did not take this course, because the system has severe security issues. Explain!

How would you design a system such that only authorized scanners will be given the registration number? How would you make sure that no one can eavesdrop to obtain the transponder reply, nor identify and track a particular car?

The problem with the first solution is that the number of possible registration numbers is so small that it is easy to perform a brute-force attack, for instance by pre-computing a table with all possible encrypted numbers (since you have the public key). It would then be a simple look-up to get the right registration number. Also, since the encryption key is public, a transponder could encrypt and send any registratation number it wants. To build a more secure system the toll station would first have to authenticate. This requires a challenge response using for example a public key scheme. When questioned, the transponder will reply with a nonce. The transponder will then sign the nonce using a private key that can be verified using a public key in the transponder. Instead of a nonce we could use a encrypted time-stamp but then we would need to have the transponders in synch with the scanners.

The system could be made more complex by having only a master public key in the transponder and the scanner sending a certificate with a temporary public key that can only be used during one day (this prevents someone from stealing a transponder and thus getting hold of the private master key). Once the toll station has been authenticated the registration number has to be sent encrypted. The encryption procedure must be different every time so that a eavesdropper cannot learn the signature of a car. This can be achieved in many ways, either by using a new secret key every time, which is delivered by the transponder using the public key of the scanner, or by introducing entropy into the encrypted information, for instance by encrypting the registration number together with a nonce.

B:8 2p. We categorize the many ways to prove who you are into four groups: Authentication due to what you know, what you are, what you have, and where you are. Identify for each of the examples below to which group the example belongs. Explain your answer.

Example 1: A passage from Hebrew Bible:
Gilead then cut Ephraim off from the fords of the Jordan, and whenever Ephraimite fugitives said, 'Let me cross,' the men of Gilead would ask, 'Are you an Ephraimite?' If he said, 'No,' they then said, 'Very well, say "Shibboleth".' If anyone said, "Sibboleth", because he could not pronounce it, then they would seize him and kill him by the fords of the Jordan. Forty-two thousand Ephraimites fell on this occasion.
—Judges 12:5-6, NJB

→ The ability to pronounce something correctly can be considered as biometric authentication.

→ "Shibboleth" is the passphrase which people have to know to pass the bridge.

Example 2: A passage from a popular story of Arabic origin: "At the end of a year Ali Baba, hearing nothing of the two remaining robbers, judged they were dead, and set out to the cave. The door opened on his saying, "Open Sesame!" He went in, and saw that nobody had been there since the Captain left it. He brought away as much gold as he could carry, and returned to town. He told his son the secret of the cave, which his son handed down in his turn, so the children and grandchildren of Ali Baba were rich to the end of their lives.
—Ali Baba and the Forty Thieves, from One Thousand and One Nights

→ "Open Sesam" is the passphrase which people have to know to enter the door.

Example 3: A European children's' story: "No," said the mother. "There is only a dirty cinder girl here. She is sitting down there in the ashes. The slipper would never fit her." She did not want to call her, but the prince insisted. So they called Cinderella, and when she heard that the prince was there, she quickly washed her hands and face. She stepped into the best room and bowed. The prince handed her the golden slipper, and said, "Try it on. If it fits you, you shall be my wife." She pulled the heavy shoe from her left foot, then put her foot into the slipper, pushing ever so slightly. It fit as if it had been poured over her foot. As she straightened herself up, she looked into the prince's face, and he recognized her as the beautiful princess. He cried out, "This is the right bride." The stepmother and the two proud sisters turned pale with horror. The prince escorted Cinderella away."
— Cinderella, from Mother Goose Stories and Grimm's Fairy Tales

→ If the shoe fits to a particular foot, the authentication is positive. This is a kind of biometric authentication.

Example 4: An episode summary of TV series where the protagonist uses a stolen badge to impersonate a police officer: Whilst looking for what Randy called "treasure" in the river after a storm, Earl found a policeman's badge which both he and Randy recognized. Earl remembered back several years ago whilst he, Randy and Joy went bowling and stole some wallets people left in their shoes whilst they played. After they left, they went to a cafe where they searched through their winnings. Earl found a police badge in one of the shoes. They decided that they needed to get rid of it, and so Earl asked for the cheque. The waitress saw the badge and, mistaking Earl for a policeman, decided not to charge him. They realized that they could use the badge to get all kinds of free things, and did so.
—"Stole a Badge", Episode 22 of Season 1 of My Name Is Earl.

→ The stolen badge can be considered as security token. (Authentication by "what you have").