NTNU
Kunnskap for en bedre verden

KANDIDAT

10183

PRØVE

TTM4135 1 Anvendt kryptografi og nettverksikkerhet

Emnekode	TTM4135
Vurderingsform	Hjemmeeksamen
Starttid	20.05.2022 07:00
Sluttid	20.05.2022 10:00
Sensurfrist	14.06.2022 21:59
PDF opprettet	15.08.2022 13:37

Cover page

Oppgave	Tittel	Oppgavetype
ℹ	Cover page	Informasjon eller ressurser

MCQ1

Oppgave	Tittel	Oppgavetype
1	MCQ1	Flervalg
2	MCQ1 justification	Tekstfelt

MCQ2

Oppgave	Tittel	Oppgavetype
3	MCQ2	Flervalg
4	MCQ2 justification	Langsvar

MCQ3

Oppgave	Tittel	Oppgavetype
5	MCQ3	Flervalg
6	MCQ3 justification	Langsvar

MCQ4

Oppgave	Tittel	Oppgavetype
7	MCQ4	Flervalg
8	MCQ4 justification	Tekstfelt

MCQ5

Oppgave	Tittel	Oppgavetype
9	MCQ5	Flervalg
10	MCQ5 justification	Tekstfelt

MCQ6

Oppgave	Tittel	Oppgavetype
11	MCQ6	Flervalg
12	MCQ6 justification	Langsvar

MCQ7

Oppgave	Tittel	Oppgavetype
13	MCQ7	Flervalg
14	MCQ7 justification	Langsvar

MCQ8

Oppgave	Tittel	Oppgavetype
15	MCQ8	Flervalg
16	MCQ8 justification	Tekstfelt

MCQ9

Oppgave	Tittel	Oppgavetype
17	MCQ9	Flervalg
18	MCQ9 justification	Tekstfelt

MCQ10

Oppgave	Tittel	Oppgavetype
19	MCQ10	Flervalg
20	MCQ10 justification	Langsvar

MCQ11

Oppgave	Tittel	Oppgavetype
21	MCQ11	Flervalg
22	MCQ11 justification	Tekstfelt

MCQ12

Oppgave	Tittel	Oppgavetype
23	MCQ12	Flervalg
24	MCQ12 justification	Tekstfelt

MCQ13

Oppgave	Tittel	Oppgavetype
25	MCQ13	Flervalg
26	MCQ13 justification	Tekstfelt

MCQ14

Oppgave	Tittel	Oppgavetype
27	MCQ14	Flervalg
28	MCQ14 justification	Langsvar

MCQ15

Oppgave	Tittel	Oppgavetype
29	MCQ15	Flervalg
30	MCQ15 justification	Langsvar

Written answer question 1

Oppgave	Tittel	Oppgavetype
31	The Autokey Cipher	Langsvar

Written answer question 2

Oppgave	Tittel	Oppgavetype
32	Feistel ciphers	Langsvar

Written answer question 3

Oppgave	Tittel	Oppgavetype
33	Computing exponentiation	Langsvar

Written answer question 4

Oppgave	Tittel	Oppgavetype
34	Corona Certificates	Langsvar

Written answer question 5

Oppgave	Tittel	Oppgavetype
35	TLS handshake protocol	Langsvar

Written answer question 6

Oppgave	Tittel	Oppgavetype

36	X3DH in Signal	Langsvar

Dummy question

Oppgave	Tittel	Oppgavetype
37	Dummy question	Muntlig

1 MCQ1

Suppose that 3^{-1} mod n = 17. Then a possible value of n is:

Select one alternative:

● 50

○ 35

○ 18

2 MCQ1 justification

Explain your answer

Fill in your answer here

GCD(3,50) = 1 and GCD(3,35) = 1, so it has to be one of those. Using back substitution we find that n=50

3 MCQ2

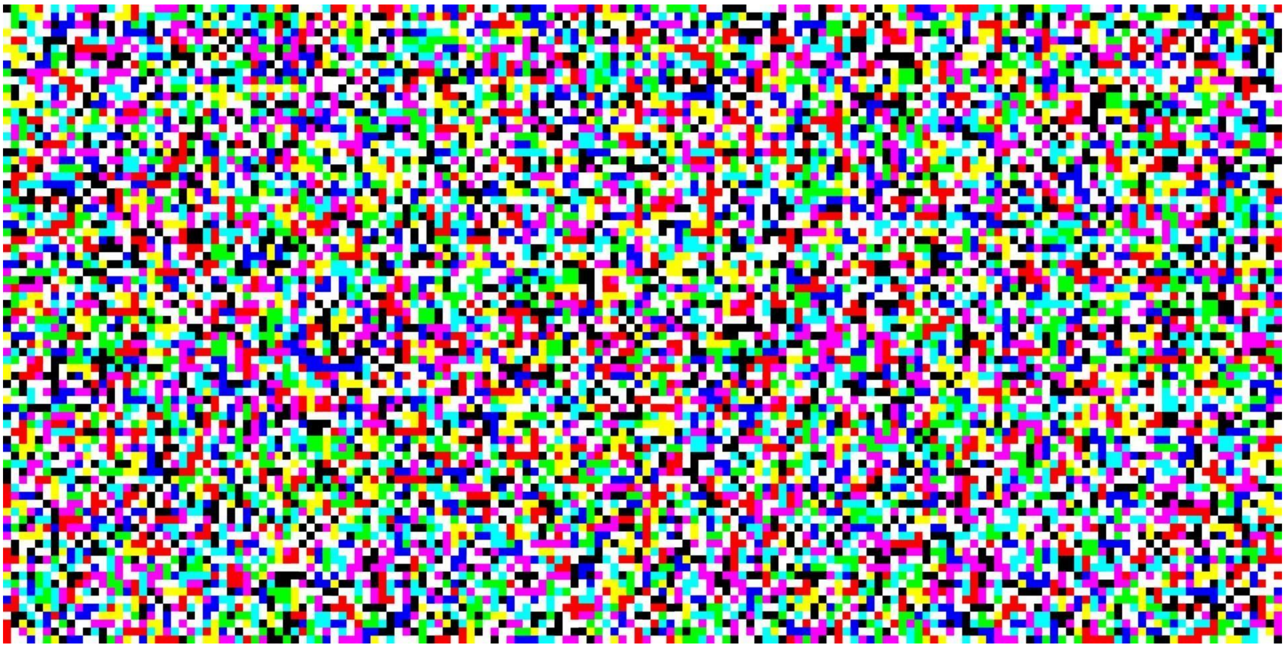


Figure A above is the result of an encryption using visual cryptography. You know that figure A is the output of a program P. You do not have access to the encryption or decryption keys, but they are encoded into P and you can run P on as many inputs as you like. You try to find out what the unencrypted figure looked like. You are performing:

Select one alternative:

○ a ciphertext only attack

○ a chosen ciphertext attack

● a chosen plaintext attack

4 MCQ2 justification

Explain your answer

Fill in your answer here

A chosen plaintext attack: can obtain the ciphertext of of some plaintext which can be selected. Can select inputs, and obtain ciphertext.

5 MCQ3

Ykg xjl'k typo tnt hddyanien xbi dbpy kwgtkibi.P

The ciphertext above is encrypted with the Hill cipher using trigrams ($d = 3$).

We decide to mount a brute force attack. How many attempts do we need at most to find the key?

Select one alternative:

○ 26^2

○ 26^3

● 26^9

6 MCQ3 justification

Explain your answer

Fill in your answer here

Since the key is a dxd size matrix the number of keys must be 26^9 keys

7 MCQ4

Suppose that you have access to two 128-bit keys, K_1 and K_2, shared with another party. You want to use the AES block cipher to provide data confidentiality for many data blocks. Which of the following options would be most secure?

Select one alternative:

○ Use AES-128 block encryption alternating between K_1 and K_2 as follows: encrypt the first block using K_1, encrypt the second block using K_2, encrypt the third block using K_1, and so on.

● Combine K_1 with K_2 by string concatenation to form K_3 of 256 bits and then encrypt all blocks with AES-256 using K_3.

○ Use AES-128 double encryption: for each block first encrypt with K_1 and then encrypt the output with K_2.

8 MCQ4 justification

Explain your answer

Fill in your answer here

Using a 256 bit key is significantly more secure than using a 128 bit key, since the keyspace increases by a factor of 2 for every new bit. For double encryption the keyspace is 2^(128) + 2^(128), while with 256 bit encryption the keyspace is 2^(128) * 2^(128)

9 MCQ5

Suppose that an active attacker observes a ciphertext of 10 blocks which was encrypted with a block cipher using some mode of operation. The attacker also knows the exact plaintext which was encrypted. The attacker wants to change the ciphertext to ensure that a specific bit in the fifth block will be flipped after decryption. Which of the following modes of operation makes this task hard for the attacker?

Select one alternative:

○ ECB mode

○ CTR mode

● CBC mode

10 MCQ5 justification

Explain your answer

Fill in your answer here

Since CBC "chains" the blocks togheter, and uses a random IV, it will be hard to change only one bit.

11 MCQ6

Why do we use *salting* when we store a password in a database?

Select one alternative:

● To make dictionary attacks from precomputed hash tables impossible, if the database is leaked.

○ Because passwords should never be stored in plaintext.

○ To make online password guessing harder.

12 MCQ6 justification

Explain your answer.

Fill in your answer here

If passwords are salted, an attacker needs to compute new hashes for all the passwords with salts, which significantly slows them down.

13 MCQ7

8911 is a Carmichael number. There are several methods to test numbers for primality. What is most likely to happen when we use them on the number 8911?

Select one alternative:

● The Fermat test outputs that 8911 is a prime, but the Miller-Rabin test disagrees

○ The Miller-Rabin test outputs that 8911 is a prime, but the Fermat test disagrees

○ The Miller-Rabin test and the Fermat test both output that 8911 is not a prime

14 MCQ7 justification

Explain your answer

Fill in your answer here

The Fermat test will output probable prime on Carmicheal numbers, but Miller-Rabin will give propable prime on composite numbers with a probability of 1/4

15 MCQ8

RSA encryption and decryption make use of a public exponent e, a private exponent d and a modulus n. For any message M with 0 < M < n, in order ensure that encryption and decryption work properly it must be true that:

Select one alternative:

● $\gcd(d,\phi(n)) = 1$

○ $\gcd(M,\phi(n)) = 1$

○ $\gcd(M,d) = 1$

16 MCQ8 justification

Explain your answer

Fill in your answer here

Since eulers function denotes the number of positive integers less and relatively prime to n.

17 MCQ9

OAEP is a coding algorithm often used together with RSA encryption. Using OAEP helps to:

Select one alternative:

○ allow longer messages to be encrypted

○ speed up decryption

● prevent attacks based on deterministic encryption

18 MCQ9 justification

Explain your answer

Fill in your answer here

OAEP adds randomness which turns RSA(deterministic) into probabilistic.

19 MCQ10

Breaking an elliptic curve-based Diffie-Hellman instantiation with curve group size p of length 256 bits is around as hard as breaking 128-bit AES — this is currently considered secure. Why are we currently investing so much into developing new cryptographic algorithms if we can just increase the group size p to length 512 bits instead?

Select one alternative:

● Because our adversaries will have access to a quantum computer in the future, and with those you can break ECDH efficiently.

○ Elliptic curve operations are always linear in the length of p, so doubling the group size only has a small effect on brute force key search.

○ We would have to keep doubling the group size every other year, as Moore’s law dictates computers will keep speeding up as well.

20 MCQ10 justification

Explain your answer

Fill in your answer here

There is no post-quantum replacement for Diffie-Hellman.

21 MCQ11

You are designing an IoT system which will turn your house's central heating on and off based on the outside temperature. Since it's IoT, everything except the server is battery-powered, and performing computations and sending data cost a lot of power.

You want to implement some security features — the temperature outside is not a secret, but you want to be sure the correct value is received, because otherwise an attacker could control your heating and increase your power bill. What do you use to protect the values you send from the thermometer to your server?

Select one alternative:

● HMAC

○ ChaCha

○ ECDSA

22 MCQ11 justification

Explain your answer

Fill in your answer here

Since HMACs comes with unforgeability, the best way is to use HMACs, it is also the cheapest computationally since you could put the symmetric keys manually on each device.

23 MCQ12

Which of the following protocol features is shared by both the Kerberos protocol *and* the TLS 1.2 handshake protocol?

Select one alternative:

● Knowledge of one session key does not compromise other session keys

○ Clients need to check the validity of the communication partner's long-term key

○ Forward secrecy is always provided

24 MCQ12 justification

Explain your answer

Fill in your answer here

TLS 1.2 does not provide foward secrecy with all cipher suites.

25 MCQ13

Two possible variants of the handshake protocol in TLS 1.2 are based on (i) RSA encryption and (ii) elliptic curve Diffie-Hellman (ECDH). The advantage of using the ECDH variant is:

Select one alternative:

● forward secrecy for the session is provided

○ the TLS *server key exchange* message is shorter

○ the handshake protocol is secure against quantum computers

26 MCQ13 justification

Explain your answer

Fill in your answer here

If an attacker gets the private key of either the client or the server, the session key can be decrypted, which makes RSA not have forward secrecy. As opposed to ECDH.

27 MCQ14

Why does TLS 1.3 remove support for non-AEAD cipher suites?

Select one alternative:

○ Because renegotiating the cipher suite used during a TLS connection is an attack vector

○ This reduces the amount of handshake messages since AEAD-cipher suites are more suitable for 0-RTT

● Because non-authenticated information in the header fields is a security risk

28 MCQ14 justification

Explain your answer

Fill in your answer here

29 MCQ15

The Double Ratchet from the Signal protocol consists of two ratcheting mechanisms.

Why is one ratchet based on Diffie-Hellman not sufficient?

Select one alternative:

○ With one ratchet we can’t support group operations in $\mathbb{Z}_p^*$ as well as in elliptic curve groups.

● With one ratchet we can’t obtain forward secrecy when there are consecutive messages from the same party.

○ We need two ratchets to obtain both authentication (through signatures) and secrecy (through encryption).

30 MCQ15 justification

Explain your answer.

Fill in your answer here

31 The Autokey Cipher

The Autokey cipher is a classical cipher invented in 1586. We start off by encrypting as we do with the Vigenère cipher, but instead of repeating the keyword, we use the plaintext as the key as follows.

Given the plaintext $p_0, p_1, \ldots$ and a key consisting of characters $k_0 \ldots k_{19}$, this means we compute the ciphertext $c_0, c_1, \ldots$ as:

$$c_i = \begin{cases} p_i + k_i \bmod 26 & \text{for } 0 \leq i < 20 \\ p_i + p_{i-20} \bmod 26 & \text{for } i \geq 20 \end{cases}$$

a) What is the key space for the Vigenère cipher? What is the key space for the Autokey cipher?

b) Do you consider this cipher to be more or less secure, compared to the Vigenère cipher?

c) What would your attack strategy be, using well-known techniques such as those from the practical assignment?

Fill in your answer here

a)
The keyspace for the Autokey cipher and the cigenere cipher is the same.

b)
The autokey cipher is more secure than the vigenere cipher, due to the non-repetive nature of the key. In the vigenere cipher the key is reapeatet k times, while the autokey cipher the key is used as generator for the keystream.

c)
Assuming the attack is a ciphertext only attack. I would use a dictionary attack, then I would look at which key length gives the most plaintext looking result. And use keys of that length to bruteforce it with a dictionary.

32 Feistel ciphers

Consider a Feistel cipher with a 160-bit block size and 14 rounds, where each round uses the Feistel construction:

- $L_i = R_{i-1}$
- $R_i = L_{i-1} \oplus f(R_{i-1},K_i)$

1. Explain, with justification, what should be the length in bits of outputs from the function f.
2. What are the possible values of the length in bits of each K_i? Of the possible lengths, state with justification what might be a reasonable choice for a practical block cipher.
3. Suppose that the function f is chosen to ignore its first input, so that we can write simply $f(R_{i-1},K_i) = f(K_i)$. Explain why the cipher is now easy to break.

Fill in your answer here

1)

2)

3)

33 Computing exponentiation

Suppose that m is an integer of 128 bits in length (so $2^{127} \le m < 2^{128}$). For some algorithm, suppose that we need to compute the exponentiation, x^e mod m, for some value x of less than 128 bits in length.

1. If m is a prime number, explain why we can always ensure that e is also of no more than 128 bits when making the computation.
2. If the square-and-multiply algorithm is used, what is the maximum number of multiplications needed? (You may assume that a squaring is the same cost as a multiplication.) Explain how you reach your answer.
3. Suppose now that m = pq where p and q are primes of 64 bits each. If the Chinese Remainder Theorem (CRT) is applied, two exponentiations are part of the computation. Show that the maximum number of multiplications is almost the same as in part 2, when the square-and-multiply algorithm is used. So why is the CRT useful?

Fill in your answer here

1)

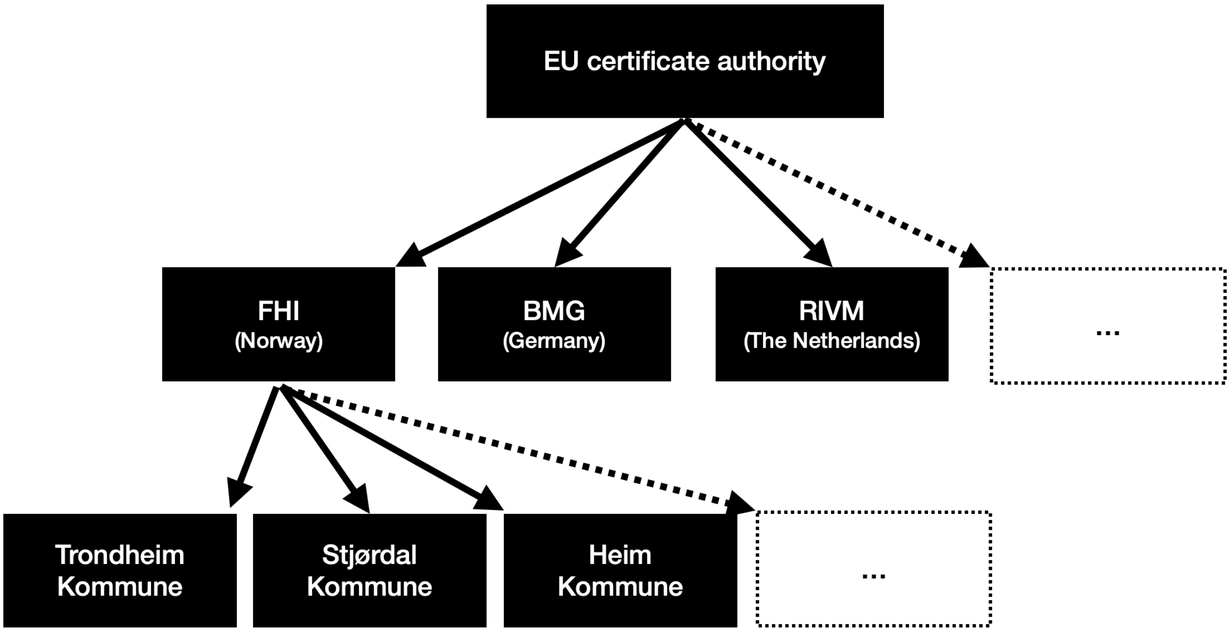
2)

3)

34 Corona Certificates

During the fall of 2021, many European countries including Norway made use of “corona passes” or “corona certificates”. In a simplified form, national authorities would sign the phrase “Person X, born Y has been vaccinated on date Z” using a government private key. This text, together with the signature, would then be turned into a QR-code which could be scanned and verified using that government’s public key.

The distributed trust system could look like this:



Eva works as a bouncer at a Trondheim night club, scanning QR-codes using the Norwegian scanning app. The app comes pre-loaded with all the public keys belonging to the Norwegian health authorities.

a) Isak got his corona shots from the Oslo municipality. Eva scans the code and confirms that the certificate is valid. What steps does her phone perform to verify this?

b) Even has a corona certificate from Germany. Eva scans the code and confirms that the certificate is valid. What steps does her phone perform to verify this?

In October 2021 the private keys belonging to the Polish government were leaked, and valid QR-codes belonging to fictitious people such as “Mickey Mouse” (born 1900) and “Sponge Bob” (born 2001) started to appear online, as well as a black market for fake yet valid QR-codes.

William buys a fake certificate on the internet for $300. The advertisement promises that the certificate will register as valid, which he verifies himself.

c) A week after purchase, William gets his QR-code scanned by Eva and is denied access. How could Eva’s phone possibly know that the code was a fake?

Fill in your answer here

a)

Evas phone gets the issues and the public key of the issues(FHI Norway) and validates the signature on the Corona Pass. As FHI can be seen as an intermediate CA, it does need to look up the root CAs public key.

b)

The same as with Isak. And since the system most likely used a non-hierarchical system, certification can be used against any CA in the system, which makes it possible to validate other countries.

c)

The system most likely used a certificate revocation list or a online certificate staus protocol. Both contains information about certificates that are revocated, and unusable. As the Polish government probably revoked the certificates for all certificates issues in a given time period.

35 TLS handshake protocol

The TLS 1.2 handshake protocol allows a client and server to agree upon various parameters to be used in both the handshake and record protocols of TLS.

1. How could a client force the server to accept the weakest ciphersuite that the server supports?
2. What will happen in the handshake protocol if the client and server do not share a ciphersuite that they both support?
3. What prevents an active attacker from forcing a client and server to use an older version of TLS, when there is a newer one that they both support?

Fill in your answer here

1.

The client can see all possible ciphersuites the server uses, using a tool such as ssllabs and choose the weakest cipher. Then the client can choose to only sent the weak ciphersuit in the ciphersuits available in the client hello. This forces the server to use the weak ciphersuit.

2.

If the client and sever do not share any ciphersuites, the sever will fail the handshake, and the client will get an error such as "Cipher suite used by client is not supported by server"

3.

36 X3DH in Signal

The Extended Triple Diffie-Hellman protocol (X3DH) is the protocol Signal uses to initialize a conversation between two parties. Signal is a privacy-centered system, so by design anyone can create an account with Signal without uploading any proof of identity. When creating an account, you upload a public identity key (IK) and a public pre-key (SPK) to the server and hold on to the private keys that correspond to these. IK is static in the long term, while SPK is replaced with a new one every week or so.

When Bob wants to talk to Alice, he gets Alice's public identity-key IK_A and a public pre-key SPK_A from the server. He then generates an ephemeral keypair EK_B and computes a shared secret SK based on four keys: the public keys IK_A and SPK_A, and the private keys corresponding to IK_B and EK_B.

Since Bob sends Alice the public keys IK_B and EK_B along with his first encrypted message, and she still has the private keys corresponding to IK_A and SPK_A, she can compute SK as well.

a) What security property/properties does Bob achieve by computing a new EK_B every time, given that he already uses his own identity key IK_B?

An adversary Charlie manages to take over the Signal servers. Charlie replaces IK_A with IK_C and SPK_A with SPK_C, before Bob starts his conversation with Alice.

b) What effect does this have on the security of the protocol? How can Bob be sure that he is actually talking to Alice, instead of Charlie?

Fill in your answer here

a)
Forward secrecy, since the key is ephemeral (keys that can only be used once).

b)
The Signal protocol uses

37 Dummy question

This task is not to be answered. It will only be used to add points from the pre-exam work.