NTNU
Kunnskap for en bedre verden

KANDIDAT

10130

PRØVE

TTM4135 1 Anvendt kryptografi og nettverksikkerhet

Emnekode	TTM4135
Vurderingsform	Hjemmeeksamen
Starttid	11.05.2021 09:00
Sluttid	11.05.2021 12:00
Sensurfrist	04.06.2021 23:59

PDF opprettet	14.07.2021 12:03

Cover page

Oppgave	Tittel	Oppgavetype
i	Cover page	Dokument

MCQ1

Oppgave	Tittel	Oppgavetype
1	MCQ1	Flervalg
2	MCQ1 justification	Tekstfelt

MCQ2

Oppgave	Tittel	Oppgavetype
3	MCQ2	Flervalg
4	MCQ2 justification	Tekstfelt

MCQ3

Oppgave	Tittel	Oppgavetype
5	MCQ3	Flervalg
6	MCQ3 justification	Tekstfelt

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	Tekstfelt

MCQ7

Oppgave	Tittel	Oppgavetype
13	MCQ7	Flervalg
14	MCQ7 justification	Tekstfelt

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	Tekstfelt

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	Tekstfelt

MCQ15

Oppgave	Tittel	Oppgavetype
29	MCQ15	Flervalg
30	MCQ15 justification	Tekstfelt

Written Answer 1

Oppgave	Tittel	Oppgavetype
31	Written Answer 1	Langsvar

Written Answer 2

Oppgave	Tittel	Oppgavetype
32	Written Answer 2	Langsvar

Written Answer 3

Oppgave	Tittel	Oppgavetype
33	Written Answer 3	Langsvar

Written Answer 4

Oppgave	Tittel	Oppgavetype
34	Written Answer 4	Langsvar

Written Answer 5

Oppgave	Tittel	Oppgavetype
35	Written Answer 5	Langsvar

Written Answer 6

Oppgave	Tittel	Oppgavetype
36	Written Answer 6	Langsvar

Dummy Question

Oppgave	Tittel	Oppgavetype
37	Dummy question	Muntlig

1 MCQ1

If x^{-1} mod 17 = 5 then

- x mod 17 = 5
- x mod 17 = 6
- x mod 17 = 7

2 MCQ1 justification

Explain your answer:

This is because 5 * 7 mod 17 = 1. Which comes from the definition of the inverse,

3 MCQ2

Suppose that the 26-letter alphabet, A,..., Z, is used for the plaintext in the 2 x 2 Hill cipher. Suppose that the letter E is the most common letter in the plaintext, occuring with frequency equal to 10%. Then in the ciphertext we can expect that:

- the most common letter occurs with frequency above 10%
- the most common letter occurs with frequency equal to 10%
- the most common letter occurs with frequency below 10%

4 MCQ2 justification

Explain your answer.

Hill cipher has a smoothing efffect on the distribution frequencies.

5 MCQ3

A typical RSA private key in use today may have length 3072 bits, but a typical symmetric key for the AES block cipher may have length only 128 bits. This longer key for RSA is necessary because:

- there are much better ways to attack RSA than brute force key search
- security for public key encryption needs to be stronger than for symmetric key encryption
- RSA keys need to be longer than symmetric keys to avoid attack by quantum computers

6 MCQ3 justification

Justify your answer.

If key distribution is done correctly, a symmetric key can be much shorter than a public key whilst giving the same degree of safety.

7 MCQ4

Suppose that in a binary synchronous stream cipher a section of the ciphertext is 01000. An attacker knows that the plaintext used to obtain this ciphertext is 00101. The corresponding section of the decryption keystream is:

- 00101
- 01000
- 01101

8 MCQ4 justification

Explain your answer

We XOR these to get the ciphertext.

9 MCQ5

Consider the version of the triple DES (3-DES) block cipher with three independent keys. Compared with the AES block cipher, this version of 3-DES:

- has a shorter block length than all versions of AES
- has fewer possible keys than all versions of AES
- is faster to run in software than all versions of AES

10 MCQ5 justification

Explain your answer.

AES uses block size of 128 whilst the 3 key 3DES (3TDEA) uses 64.

11 MCQ6

Suppose that you have a message of 100 bits to encrypt and you choose to use the AES block cipher. Which of the following modes of operation will require the least number of sent bits in the encrypted message?

- ECB mode
- Counter mode with a nonce of 64 bits
- CBC mode

12 MCQ6 justification

Explain your answer:

CTR mode does not require padding so we do not need to send more bits than the original 100.

13 MCQ7

The Euler function ϕ is often useful for public key cryptography. It is true that:

- if n is divisible by 3 then $\phi(n)$ is always divisible by 3
- $\phi(n)$ is always divisible by 3
- if n is divisible by 9 then $\phi(n)$ is always divisible by 3

14 MCQ7 justification

Explain your answer.

p = 3, q = 2, n = 6, o(6) = 2

n is divisible by 3, bun not o(n).
o(n) is not divisible by 3.

however:

if n is divisible by 9 we will in calculating euler function get 3^e as a factor where e>1. Then when caculated we will have in calculation of o(n) in the product 3^(e-1) and as e >1 we wlll always have a 3 as a factor.

15 MCQ8

Suppose you want to prevent an attacker from finding a collision in a hash function. The attacker has enough computing power to calculate 2^{40} hash values. You need to ensure that the attacker has only small chance of success but prefer the smallest acceptable output size. You have three possible output sizes to choose from. Which should you choose?

- 64 bits
- 128 bits
- 40 bits

16 MCQ8 justification

Explain your answer.

By the birthday paradox, we have that the attacker has the power to make (2^40)^2 = 2^80 be unsafe. Therefore I choose the smallest amount of bits larger than this from the multiple choice alternatives.

17 MCQ9

A message authentication code, MAC, takes as input a key K and message M and outputs a tag T. In order to be secure, it is essential that:

- [x] an attacker who knows a valid M and T cannot find K
- [ ] an attacker who knows a valid K and T cannot find M
- [ ] an attacker who knows a valid K and M cannot find T

18 MCQ9 justification

Explain your answer.

The K is the secret key and should only be known to the valid users, and it should be infeasible to reverse MAC to find the key from a message and tag.

19 MCQ10

The RSA signature scheme uses a modulus n and a public exponent e. If the modulus is chosen to be n = 13 x 23 = 243 then the smallest valid choice for e would be:

- [ ] e=3
- [x] e=5
- [ ] e=7

20 MCQ10 justification

Explain your answer.

I'm assuming you mean 13 * 23 = 299.

This give euler(n) = 12*22 = 264

The smallest valid choice for e is in general 3 but is not valid here as 3 is not invertible modulo 264.

Therefore 5 is the smallest valid choice for e as it is valid for n = 299.

21 MCQ11

For efficiency reasons it is often useful to keep fixed parameter values for many users of a cryptographic scheme. Which of the following is **not** a practical choice for digital signatures?

- RSA signatures with a fixed modulus n
- DSA signatures with fixed generator g and fixed modulus p
- ECDSA signatures with a fixed elliptic curve group

22 MCQ11 justification

Explain your answer.

The signature size should vary, but in ECDSA we have a fixed signature size.

23 MCQ12

When assessing the security of a key establishment protocol, such as the Needham--Schroeder protocol, we assume that an attacker is able to:

- force parties to re-use nonces used in previous runs of the protocol
- re-send messages sent in any previous runs of the protocol
- obtain long-term keys used in any previous runs of the protocol

24 MCQ12 justification

Explain your answer.

This makes sure we check whether the protocol is vulnerable to replay attacks.

25 MCQ13

In the TLS 1.2 handshake protocol, a ciphersuite is negotiated between the client and the server. Which of the following does **not** depend on the chosen ciphersuite:

- the algorithm used to sign the server certificate
- the algorithm used to authenticate the record layer data
- the algorithm used to sign the server key exchange message

26 MCQ13 justification

Explain your answer.

The algorithm used to sign the server certificate does not depend on the ciphersuite, as this is not something that the server or client signs.

27 MCQ14

TLS 1.3 aims to establish secure connections faster than TLS 1.2. One difference between the protocols which contributes to this is:

- checking of server certificates is not required
- clients can send a Diffie--Hellman ephemeral value before the ciphersuite is agreed
- servers can initiate the handshake protocol and use a ciphersuite of their choice

28 MCQ14 justification

Explain your answer.

The keyshare is done during the client hello in an optimistic manner assuming that its ciphersuite is acceptable to the server. This is done to reduce the total RTT's necessary.

29 MCQ15

PGP is a security protocol to protect emails in transit. PGP has seen very limited usage in practice. One of the reasons for this is:

- PGP-encrypted mail cannot be sent on the normal email system
- usability is a challenge for many potential users
- encryption is provided but it is not possible to authenticate mail senders

30 MCQ15 justification

Explain your answer.

A lot of the potential users do not have the knowledge necessary to understand pulic key cryptography as it is quite complex. One cannot expect every average joe to sit down and learn cryptography before sending an email. Many people just don't see the time investment as valid when their emails are generally mundane and unimportant.

31 Written Answer 1

Suppose that you share a new (unused) random key of 128-bits with a recipient. You are considering whether to use the key either as a one-time pad or with the AES block cipher in ECB mode.

1. Suppose first that you have a single message to encrypt, written in English as 16 x 8-bit bytes to make 128 bits in total. For this part assume that the key is used only once for this message. Compare the security of each of the two choices. Is one better than the other and why?
2. Now suppose that you have a second message to encrypt, also written in English as 16 x 8-bit bytes. You decide to use the same encryption method with the same key as you used for the first 128-bit message. Again, compare the security of the two choices.

1

Here we would use one time pad as this provides perfect secrecy. Which we do not get from AES block cipher in ECB mode. Therefore OTP is better.

2.

Now that the key is to be reused, the one time pad is not longer perfectly secret. This is because we need to have the same amount of keys as messages. Thus the OTP is not much better than the Vigenere, and AES ECB is much better.

32 Written Answer 2

The Feistel construction for a block cipher uses the round equations:
$L_i = R_{i-1}$
$R_i = L_{i-1} \oplus f(R_{i-1},K_i)$
for some function f. Suppose that f is chosen to be the function $f(R,K) = R \oplus K$, for any half-block, R, and any round key, K.

- Show that with this choice of f it follows that for all i > 1, both of the following equations hold.

$R_i = L_{i-2} \oplus K_{i-1} \oplus K_i$
$L_i = L_{i-2} \oplus R_{i-2} \oplus K_{i-1}$

- Use the above observation to show how to break a 2-round Feistel cipher with this f

function given one known plaintext/ciphertext pair.
- Explain, just giving the idea, how this can be generalised to break a Feistel cipher with any even number of rounds if this f function is used.

1

$r_i = L_{i-1}$ XOR $(R_{i-1}$ XOR $k_i)$

$L_i = R_{i-1}$

$L_{i-1} = R_{i-2}$

$R_{i-1} = L_{i-2}$ XOR $(R_{i-2}$ XOR $K_{i-1})$

putting back into:

$R_i = R_{i-2}$ XOR $(L_{i-2}$ XOR $(R_{i-2}$ XOR $K_{i-1})$ XOR $K_i)$ $= R_{i-2}$ XOR L_{i-2} XOR R_{i-2} XOR K_{i-1} XOR K_i

$R_i = L_{i-2}$ XOR K_{i-1} XOR K_i

$L_i = R_{i-1} = L_{i-2}$ XOR R_{i-2} XOR K_{i-1}

2:

We can break the two round cipher because that the XOR is its on inverse and therefore removes terms.

As we see, R_i is dependent only on the round keys and the plaintext L. This

combined with that the L_i is dependent only on one round key and the plaintext. Given a known plaintext/ciphertext pair, we kan find K_i-1 by the L-expression, and using the found k_i-1, we can find k_i from the R-expression, as we know the plaintext, the ciphertext and the round key k_i-1. Therefore k_i is the only unknown and we kan find it trivially.

3:

As the XOR is its own inverse function, applying it a even amount of times is dangerous as it cancels itself out. Therefore using this function will leave one side as an expression of the XOR of the keys and the opposite plaintext part. The attacker can then with a n-1, where 2n is the amount of rounds, ciphertext/plaintext pairs break the cipher by working backwards taking out one after another.

33 Written Answer 3

One non-trivial square root of 1 modulo 209 is 153.

1. What are all four of the square roots of 1 modulo 209?
2. Choose one of your non-trivial square roots, x and show, using the Euclidean algorithm, that gcd(x+1,209) > 1.
3. Explain how an efficient algorithm to find non-trivial square roots can be used to break the RSA cryptosystem.

1

The four square roots are the two trivial and two non-trivial.
trivials: 1 and -1, giving (mod 209) 1 and 208.
non-trivials: 153 (given), and -153, giving (mod 209) 153 and 56
in total, the square roots og 1 modulo 209 are: {1, 56, 153, 208}

2:

Choosing 56+1 = 57
209 = 3*57 + 38
57 = 1 * 38 + 19
38 = 19*2

gcd(57, 209) = 19

3:

By finding non-trivial square root, we can find the prime factors, which then again would break RSA.

34 Written Answer 4

The normal RSA cryptosystem uses modulus n = pq, a decryption exponent, d, and public exponent, e. Suppose that a company wants to protect its private exponent so that no single entity can decrypt. The manager splits d into two parts, d1, d2 such that d1 + d2 mod ϕ(n) = d, and gives d1 to entity E_1 and d2 to entity E_2.
In order to decrypt a ciphertext C, entity E_1 computes $M_1 = C^{d1}$ mod n, entity E_2 computes $M_2 = C^{d2}$ mod n and then these are combined to form $M = M_1 \times M_2$ mod n.

1. Show that a ciphertext encrypted with normal RSA, with public key e and n, is decrypted properly with this method. (You may assume that normal RSA works correctly.)
2. To improve the efficiency the manager decides to give both E_1 and E_2 the values p and q so that they can use the Chinese Remainder Theorem to decrypt.
    - Does this make the decryption as fast as normal RSA? Explain your answer.
    - Why does this defeat the purpose of the system?

1

n = p*q

M1 = C^d1 mod n

M2 = C^d2 mod n

M = M1 * M2 mod n

$= C^{d_1} \cdot C^{d_2} \ mod \ n$

$= C^{d_1 + d_2} \ mod \ n$

$= C^{d_1 + d_2 \ mod \ \theta(n) + k \cdot \theta(n)} \ mod \ n$

$= C^{d_1 + d_2 \ mod \ \theta(n)} \cdot C^{k \cdot \theta(n)} \ mod \ n$

$= C^{d} \cdot 1 \ mod \ n$

= M

2

CRT increases efficiency by a factor of 4. Given that the sending between entities is instant and no other overhead is endured, this decryption with CRT is faster than regular RSA decryption without CRT by a factor of two.

As the decryption is uses half the time of decryption, brute force will also use half the time to guess one of them. Having two "keys" d_1 and d_2 increases the difficulty by a factor of two, but with the decreased decryption time by a factor of two cancels out the point of having two keys.

35 Written Answer 5

Consider the following protocol with the goal of key establishment. This is a repaired version of the Needham--Schroeder protocol.

Here N_A is a nonce chosen by party A, N_B is a nonce chosen by B, and K_{AB} is the session key chosen by server S. ID_A and ID_B are identity strings for A and B respectively. K_AS and K_BS are key-encrypting keys initially shared between S and A, and between S and B respectively. The notation $\{X\}_K$ denotes authenticated encryption of X with key K.

1. $A \rightarrow B$: ID_A, N_A
2. $B \rightarrow S$: ID_A, ID_B, N_A, N_B
3. $S \rightarrow B$: $\{N_A, ID_A, ID_B, K_{AB}\}_{K\_AS}$, $\{N_B, ID_A, ID_B, K_{AB}\}_{K\_BS}$
4. $B \rightarrow A$: $\{N_A, ID_A, ID_B, K_{AB}\}_{K\_AS}$

1. On receipt of message 4, A should check that the received N_A is the same value as that chosen in message 1. Describe an attack on the protocol if A does not perform this check, including the messages which an attacker sends. What is the consequence of this attack?
2. Suppose that instead of using authenticated encryption, plain encryption by a synchronous stream cipher is used, such as AES in counter mode. How does this also allow an attack?

Skriv ditt svar her

1

If A does not check N, any other entity C which obtains a previously established session key between A and B, can masquerade as A. The consequence of such an attack is that C (masquerading as A) can persuade B to use the old session key which C has obtained.

2

The problem with counter mode is that it is malleable. An attacker can alter the ciphertext without detection, and then pass on. Then the recipient would decrypt the ciphertext altered by the attacker.

A mode like GCM would be better suited as it authenticates the message making it impossible to alter the sent encrypted MSG without being detected.

36 Written Answer 6

The Signal messaging protocol uses two kinds of *ratcheting* to update the keys used to protect messages: Diffie--Hellman ratcheting is used when the next message is sent in the opposite direction from the previous message; symmetric ratcheting with a hash function is used when the next message is sent in the same direction.
Assume a powerful adversary who can capture and delay messages and has the ability to compromise devices later.

1. How does the ratcheting in Signal improve the security of messages against this adversary, in comparison to the security of:
    - email messages encrypted with PGP;
    - messages sent as application data in a TLS 1.3 session.
2. If several messages are sent in the same direction in the Signal protocol, how does

their security compare to the security of messages sent successively in opposite directions?

Skriv ditt svar her

1

In PGP, the messages to a recipient are encrypted with the same public key over and over again. In contrast to this, Signal uses ephemeral key exchanges for each session. This is important because an attacker who records ciphertexts sent over the network can later decrypt all of them if the manage to break the single key used. This is why Signal is better in this usage.

2

When several messages are sent in the same direction in the Signal protocol, the key is updated with a symmetric ratchet. When we sent in opposite directions we create a new message key with a DH ratchet. The security is not much different other than the difference between Diffie hellman and the symmetric employed in local ratcheting.

37 Dummy question

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