TTM4135 exam May 2022: Outline answers

1 Multiple choice questions

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

   (a) $n = 18$
   (b) $n = 35$
   (c) $n = 50$

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

   (a) A chosen ciphertext attack
   (b) A chosen plaintext attack
   (c) A ciphertext only attack

3. 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?

   (a) 26^3
   (b) 26^2
   (c) 26^9

4. 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?

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

   (b) Combine K_1 with K_2 by string concatenation to form K_3 and then encrypt all blocks with AES-256 using K_3.

   (c) Alternate AES-128 block encryption with K_1 and K_2 as follows: encrypt block 1 using K_1, encrypt block 2 using K_2, encrypt block 3 using K_1, and so on.

5. 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?

   (a) ECB mode

   (b) CBC mode

   (c) CTR mode

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

   (a) To make online password guessing harder.

   (b) To make dictionary attacks impossible, if the database is leaked.

   (c) Because passwords should never be stored in plaintext.

7. 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?

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

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

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

8. RSA encryption of a message M makes use of a public exponent e, a private exponent d and a modulus n. To ensure that encryption and decryption work properly it must be true that:

   (a) $\gcd(M, d) = 1$

   (b) $\gcd(\phi(n), d) = 1$

   (c) $\gcd(M, \phi(n)) = 1$

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

   (a) prevent attacks based on deterministic encryption

   (b) allow longer messages to be encrypted

   (c) speed up decryption

10. 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?

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

    (b) 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.

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

11. 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?

    (a) HMAC

    (b) ECDSA

    (c) Chacha

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

    (a) Forward secrecy is always provided

    (b) Knowledge of one session key does not compromise other session keys

    (c) Clients need to check the validity of the communication partner's long-term key

13. 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:

    (a) the TLS server key exchange message is shorter

    (b) the handshake protocol is secure against quantum computers

    (c) forward secrecy for the session is provided

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

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

    (b) This reduces the amount of handshake messages since AEAD ciphersuites are more suitable for 0-RTT

    (c) Because non-authenticated information in the header fields is a security risk

15. The Double Ratchet from the Signal protocol consists of two ratcheting mechanisms. Why is one ratchet based on Diffie-Hellman not sufficient?

    (a) With one ratchet we can't obtain forward secrecy when there are consecutive messages from the same party.

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

    (c) With one ratchet we can't support group operations in as well as in elliptic curve groups.

2 Written answer questions

1. 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 as:

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

1. What is the key space for the Vigenère cipher? What is the key space for the Autokey cipher?
2. Do you consider this cipher to be more or less secure, compared to the Vigenère cipher?
3. What would your attack strategy be, using well-known techniques such as those from the practical assignment?

2. Feistel ciphers Consider a Feistel cipher with a 128-bit block size, a 128-bit key, and 16 rounds. Each round uses the Feistel construction:

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

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, suggest 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.

3. Exponentiation Suppose that m is an integer of 100 bits in length (so $2^{99} \leq m < 2^{100}$). For some algorithm, suppose that we need to compute the exponentiation

$$x^e \bmod m$$

for some value x of less than 100 bits in length.

1. If m is a prime number, explain why we can always assume that e is also of no more than 100 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 50 bits each. If the Chinese Remainder Theorem (CRT) is applied for the computation, two exponentiations are computed. Show that the maximum number of multiplications is almost the same as the previous part of this question when the square-and-multiply algorithm is used. So why is the CRT useful?

4. 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.

(Picture of hierarchical certification tree omitted.)

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?

5. TLS Handshake 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?

6. X3DH 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.

1. 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?

2. 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.

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?