NTNU – Trondheim
Norwegian University of
Science and Technology

Department of Information Security and Communication Technology

Examination paper for TTM4135 Applied Cryptography and Network Security

Academic contact during examination: Colin Boyd

Phone: 98065197

Examination date: 2023-06-08

Examination time (from-to): 09:00 - 12:00

Permitted examination support material: (D) No printed or hand-written support material is allowed. A specific basic calculator is allowed.

Other information: –

Language: English

Number of pages: 4

Number of pages enclosed: 0

Checked by:

Date Signature

TTM4135 Spring exam 2023:
Outline answers

Exercise 1 Multiple choice questions

1.	(a) ☐	(b) ☑	(c) ☐	(d) ☐
2.	(a) ☐	(b) ☑	(c) ☐	(d) ☐
3.	(a) ☐	(b) ☐	(c) ☐	(d) ☑
4.	(a) ☑	(b) ☐	(c) ☐	(d) ☐
5.	(a) ☐	(b) ☑	(c) ☐	(d) ☐
6.	(a) ☐	(b) ☐	(c) ☑	(d) ☐
7.	(a) ☐	(b) ☐	(c) ☑	(d) ☐
8.	(a) ☑	(b) ☐	(c) ☐	(d) ☐
9.	(a) ☑	(b) ☐	(c) ☐	(d) ☐
10.	(a) ☐	(b) ☑	(c) ☐	(d) ☐
11.	(a) ☐	(b) ☐	(c) ☐	(d) ☑
12.	(a) ☐	(b) ☑	(c) ☐	(d) ☐
13.	(a) ☐	(b) ☑	(c) ☐	(d) ☐
14.	(a) ☐	(b) ☐	(c) ☑	(d) ☐
15.	(a) ☐	(b) ☐	(c) ☑	(d) ☐
16.	(a) ☐	(b) ☐	(c) ☑	(d) ☐
17.	(a) ☐	(b) ☐	(c) ☐	(d) ☑
18.	(a) ☑	(b) ☐	(c) ☐	(d) ☐
19.	(a) ☐	(b) ☐	(c) ☐	(d) ☑
20.	(a) ☑	(b) ☐	(c) ☐	(d) ☐
21.	(a) ☐	(b) ☑	(c) ☐	(d) ☐
22.	(a) ☐	(b) ☐	(c) ☐	(d) ☑
23.	(a) ☐	(b) ☐	(c) ☑	(d) ☐
24.	(a) ☐	(b) ☐	(c) ☐	(d) ☑

25.	(a) ☐	(b) ☐	(c) ☑	(d) ☐
26.	(a) ☑	(b) ☐	(c) ☐	(d) ☐
27.	(a) ☐	(b) ☐	(c) ☑	(d) ☐
28.	(a) ☐	(b) ☐	(c) ☐	(d) ☑
29.	(a) ☑	(b) ☐	(c) ☐	(d) ☐
30.	(a) ☐	(b) ☐	(c) ☑	(d) ☐

Exercise 2 Written answer questions

1. (a) The 3x3 Hill cipher is a simple substitution on trigrams. Therefore the most common trigrams in the plaintext will also occur as common trigrams in the ciphertext. This will hold precisely with non-overlapping counts. With overlapping counts the distribution will be flatter because the most prominent trigrams will not be encrypted the same way 2 out of every 3 occurences.

   The random simple substitution will change each common digram to a different trigram which will occur with the same frequency. This the same for both overlapping and non-overlapping counting.

   The transposition cipher will move the 3 letters of each trigram into different positions and thus will disperse the common trigrams into many different trigrams. Therefore the distribution of trigrams will be much smoother.

   (b) The most common plaintext trigrams can be used to find good candidates for plaintext-ciphertext pairs. There is a good probability to be able to correctly guess the ciphertext for common words such as THE and AND. When these are guessed correctly the key matrix can be found by solving the linear equation $K = CP^{-1}$ as long as the P matrix is invertible. If not, or of the guesses turn out to be incorrect, then further candidate trigrams should be used.

2. (a) A good block cipher will have avalanche properties so that change of one input but will randomly change the output bits. More generally, we expect block ciphers to give random looking output whatever the values of the key and plaintext.

   (b) All of the output blocks, both before and after time t, can be recovered once one state and the key are revealed. This is because incrementing S_t is easily done and reversed by the attacker. Note that this is meant for a standard DRBG, so the full definition, including the hash function, will be known to any attacker.

   (c) Now revealing one state will allow output to be computed forward both inside the current set of 100 blocks and beyond in the forward direction. However, due to the one-wayness of the hash function, output before the last change of key will not be available to the attacker.

3. (a)

$$\begin{aligned} M_1 M_2 \bmod n &= C^{d_1} C^{d_2} \bmod n \\ &= C^{d_1+d_2} \bmod n \\ &= C^{d} \bmod n \\ &= M \bmod n \end{aligned}$$

   where the third line applied Euler's theorem and the last line is simply the normal RSA decryption.

   (b) The value d_1 is chosen randomly modulo n, and the value d_2 is chosen from knowing d_1. This is a bit like a one-time pad, so that knowing one of d_1 and d_2 still leaves almost all numbers possible for the other one, on the assumption that d is random. Strictly speaking, d_2 is leaking some small information about $\phi(n)$. However, a roughly correct argument is that both d_1 and d_2 are random. Note that brute force key search is not relevant in this question – factorisation of the modulus is the best (known) attack on RSA and in case case all of d, d_1 and d_2 are expected to have the same size.

(c) Using the system as specified in the question, the CRT cannot be used because it requires knowledge of the factors of n which is equivalent to knowledge of d. Thus the CRT could only be used if both managers have the ability to recover d, which would take away the point of the setup since now each manager can decrypt separately.

4. (a) An ECDSA key cannot be used with RSA key transport, since the client needs to use an RSA public key. For signed Diffie-Hellman the signature can be added with either an RSA or an ECDSA signature. So a server can get away with a single RSA public key if it uses it for both signatures and encryption (arguably bad security practice but widely seen in practice). RSA key transport can be much more efficient in computation for the client due to a short public exponent, but (when used with Diffie-Hellman handshake) RSA signatures are much longer than ECDSA signatures. ECDSA public keys are also shorter than RSA public keys which can influence the server certificate size.

   (b) TLS 1.3 does not allow RSA key transport so there is no problem not to have an RSA key for signatures (although it is certainly possible). In addition TLS 1.3 requires support for elliptic curve Diffie-Hellman so servers are already going to have elliptic curve cryptography implemented and it reduces the computational assumptions to use ECDSA signatures rather than having RSA signatures to sign ECDH.

5. (a) The main issue here is whether the pre-distributed keys should be classed as ephemeral keys or long-term keys. In practice they are available for around 2 weeks, so they do not fit the typical longevity of either. Their use is definitely a downgrade from using ephemeral keys which exist only for the duration of the key exchange protocol. However, some degree of forward secrecy is supplied because after the pre-distributed keys are replaced they are no longer available to an attacker who compromises the server.

   (b) Compromise of the current state allows an attacker to find future keys when they are updated only by hashing. Earlier keys cannot be revealed, whether in the same hash chain (same direction) or using an earlier Diffie-Hellman key. After a message is sent in reply (opposite direction), the Diffie-Hellman chain will be resumed and a passive attacker will lose ability to obtain message keys.