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: Anamaria Costache

Phone: 98065197

Examination date: 2025-08-07

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: 3

Number of pages enclosed: 0

Checked by:

Date Signature

TTM4135 August exam 2025:
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) There are n^4 possible 2×2 matrices modulo n. The set of all possible keys are the set of all such invertible matrices.
   (b) In a chosen plaintext attack the attacker can choose a plaintext (matrix P for the Hill cipher) and see the corresponding ciphertext (matrix C).
   In a chosen ciphertext attack the attacker can choose a ciphertext C and see the corresponding plaintext P.
   (c) A ciphertext-only attack can be run as follows: the Hill cipher encryption, preserves some digrams from the plaintext in the ciphertext. If the ciphertext is long enough, some groups of letters appear more often than others. We can then assume that those match to the most common digrams in the English language and construct plaintext-ciphertext pairs. Then we might be able to recompute the key via $K = CP^{-1}$.
2. (a) Encryption is now deterministic so every message always encrypts to the same ciphertext. In particular the first block now always encrypts the same way. An attacker can mount a dictionary attack using known or chosen plaintext attacks and decrypt blocks in the dictionary.
   (b) A one-bit change to the ciphertext results in incorrect decryption of the corresponding block, and of the following one. But the remaining blocks remain intact.
   (c) Encryption cannot be done in parallel, but decryption can.
3. (a) $M_p = C^{5 \bmod 4} \bmod 5 = 2^1 \pmod 5 = 2$
   $M_q = C^{5 \bmod 12} \bmod 13 = 2^5 \pmod{13} = 6$
   (b) $M = (2 \times 13 \times 13^{-1} \pmod 5) + (6 \times 5 \times 5^{-1} \pmod{13}) \pmod{65} = 32.$
   (c) Yes; we are running computations modulo p and q which are roughly half the size of n, instead of running computations modulo n.
4. (a) Listing all values is okay, else using Fermat's theorem is also ok.
   (b) The shared key they obtain is $s = y^a \pmod p = 5^8 \pmod{11} = 4$.
5. (a) Forward secrecy prevents future compromises of secret keys from past sessions.
   (b) It can only accept ciphersuites that ensure this (during the handshake protocol).
   (c) 0-RTT, faster connection, more secure ciphersuites, mandatory forward secrecy.