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

Academic contact present at the exam location: No

Phone: 98065197

Examination date: 2024-08-15

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 2024:
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) $\phi(\omega) \cdot \omega$ – since we must have $\gcd(a, \omega) = 1$, there are $\phi(\omega)$ possible values for a, and ω possible values for b.
   (b) For $\omega = 28$, $\phi(\omega) \cdot \omega = 336$.
   (c) 19.
2. (a) $P_t = C_t \oplus O_t$.
   (b) No (but keystream can be computed in advance)
   (c) No
   (d) A one-bit change in the ciphertext produces a one-bit change in the plaintext at the same location.
3. (a) i. If $\sigma = \texttt{Sig}(m, K_s)$, then $\texttt{Ver}(m, \sigma, K_v) = \texttt{True}$, for any matching signing/ verification keys
      ii. It is computationally infeasible for anyone without K_s to construct m and σ such that $\texttt{Ver}(m, \sigma, K_v) = \texttt{True}$.
   (b) Can forge signatures: for any two m, m', where an attacker can obtain the respective signatures σ, σ', the signature $\sigma \cdot \sigma'$ is a valid signature for the message $m \cdot m'$.
   (c) Hash the message before inputting it into the signature algorithm.
4. (a) They can list all values, or use Fermat's little theorem – all answers are accepted here.
   (b) $b = 4$. Partial credit if they explain methodology/ how to get the answer/ etc., even if the correct value is not recovered.
5. (a) The client does authenticate themselves, and so the server cannot verify their identity.
   (b) – Advantages: flexibility, backwards compatibility.
      – Disadvantage: downgrade attacks.
   (c) The advantage is that we can have a faster connection. The disadvantage is that it can enable certain types of replay attacks.