NTNU | Norwegian University of Science and Technology

COURSE SUMMARY

TTM4135 – Exam Review Lecture

Emil August Hovd Olaisen

27.04.2026

Motivation

- We summarize core concepts, security properties, and common failures
- Focus is on assumptions and correct use of cryptographic primitives
- Emphasis is placed on reasoning and system-level security

Security Goals

- Confidentiality: preventing unauthorized disclosure
- Integrity: preventing unauthorized modification
- Authenticity: verifying identities and data origin
- Non-repudiation: preventing denial of performed actions
- Availability: ensuring systems remain usable

Threat Models

- Passive attackers: eavesdropping only
- Active attackers: modifying, injecting, or replaying messages
- Security guarantees are always relative to a defined threat model

Historic Cryptography

- Early ciphers relied on simple transformations with limited key spaces
- Examples include Caesar, substitution, Hill, and Vigenère ciphers
- These schemes are vulnerable to statistical and known-plaintext attacks
- Their value today is pedagogical rather than practical

Symmetric Cryptography

- Uses a shared secret key between communicating parties
- Very efficient for encrypting large amounts of data
- Key distribution, not computation, is the main challenge

Stream Ciphers

- Generate a pseudorandom keystream that is XORed with the plaintext
- The keystream must be unpredictable and never reused
- Reusing a keystream leaks information about plaintexts
- The One-Time Pad is perfectly secure but impractical

Block Ciphers

- Deterministic encryption of fixed-size blocks under a given key
- Security achieved through confusion and diffusion
- Not secure on their own for encrypting multi-block messages
- AES is the modern standard; DES is not recommended today

Modes of Operation

- Define how block ciphers are used to encrypt long messages
- ECB leaks structure and must never be used
- Secure modes require randomness (IVs or nonces)
- Examples include CBC, CTR, and GCM

Hash Functions

- Map arbitrary-length input to a fixed-length output
- Security properties include collision, preimage, and second-preimage resistance
- Merkle–Damgård based hash functions are vulnerable to length-extension attacks

Message Authentication Codes (MACs)

- Provide integrity and authenticity of messages
- Require a shared secret key
- Attacks include existential and selective forgery
- HMAC prevents length-extension attacks
- MACs do not provide non-repudiation

Authenticated Encryption

- Combines confidentiality and integrity
- Encrypt-then-MAC is a secure generic composition
- AEAD schemes integrate both securely
- Examples include AES-GCM and ChaCha20-Poly1305

Chinese Remainder Theorem

The Chinese Remainder Theorem states that congruences modulo pairwise coprime integers have a unique combined solution modulo their product.

It is used in RSA implementations to speed up decryption and signing.

Finite Fields

- A finite field contains a finite number of elements
- $\mathbb{Z}_p$ is a field if and only if p is prime
- $\mathbb{Z}_p^*$ is the multiplicative group modulo p
- Elliptic curves are defined over finite fields, commonly $\mathbb{F}_p$ and $\mathbb{F}_{2^m}$

Euler's Totient Function

- $\phi(n)$ counts integers that are invertible modulo n
- If $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$
- Central to the correctness of RSA

Hard Computational Problems

- Integer factorization and discrete logarithm problems
- Cryptographic security depends on parameter sizes and the best known algorithms for attacking the schemes
- Miller–Rabin is a widely used probabilistic primality test

Key Exchange

- Allows shared secrets to be established without prior agreement
- Diffie–Hellman enables this but provides no authentication
- Authentication is required to prevent man-in-the-middle attacks

Authentication Protocols

- The goal is to verify identity, not secrecy
- Challenge–response protocols use freshness to prevent replay attacks
- Password-based authentication is error-prone if poorly designed

Digital Signatures

- Provide integrity, authenticity, and non-repudiation
- Typically implemented using a hash-then-sign construction
- Do not provide confidentiality on their own

Public Key Infrastructure (PKI)

- Certificates bind identities to public keys
- Certificate Authorities establish trust relationships
- TLS relies on PKI for server authentication

Replay Attacks and Freshness

- Replay attacks reuse previously valid messages
- Prevented using nonces, timestamps, or sequence numbers
- Essential for authentication and key exchange protocols

Forward Secrecy

- Limits damage from long-term key compromise
- Past session keys remain secure even if long-term keys are exposed
- Used in TLS and modern secure messaging systems

Post-Quantum Cryptography

- Shor's algorithm breaks RSA and discrete-log-based cryptosystems
- Lattice-based schemes are strong post-quantum candidates
- Several countries recommend hybrid deployments

Learning With Errors (LWE)

- LWE is a hardness assumption based on noisy linear equations
- The problem is given by

$$\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \pmod{q}$$

  where $\mathbf{s}$ is a secret vector and $\mathbf{e}$ is a small error vector
- The error term prevents solving the system using standard linear algebra
- LWE is believed to be secure against both classical and quantum attacks
- ML-KEM and ML-DSA are NIST post-quantum standards based on lattice assumptions for key exchange and signatures, respectively

Transport Layer Security (TLS)

- Uses a handshake phase to establish shared keys
- The record layer encrypts and authenticates application data
- TLS 1.3 removes legacy algorithms and insecure configurations

Secure Messaging

- Requires asynchronous secure communication
- End-to-end encryption protects data from service providers
- Signal provides forward secrecy and post-compromise security

Encrypted Email

- Email uses asynchronous, store-and-forward communication
- TLS protects emails only between mail servers, not end-to-end
- End-to-end encrypted email uses public-key cryptography such as PGP
- Provides confidentiality and authenticity, but has usability and key management challenges