Cryptography Engineering

- Lecture 13 (Feb 12, 2025)

- Today: Summary

Cryptography Engineering

- Symmetric-key primitives
  - SHA, AES, AES-GCM, AEAD, HMAC, HKDF, …

Cryptography Engineering

- Symmetric-key primitives
- MitM, Signature (ECDSA), Certificate, Reuse attack on DSA

Cryptography Engineering

- Symmetric-key primitives
- MitM, Signature (ECDSA), Certificate, Reuse attack on DSA
- Signed Diffie-Hellman Key Exchange, TLS handshake, “Everything-over-TLS”

Cryptography Engineering

- Symmetric-key primitives
- MitM, Signature (ECDSA), Certificate, Reuse attack on DSA
- Signed Diffie-Hellman Key Exchange, TLS handshake, “Everything-over-TLS”
- Secure Messaging, X3DH (allows two users perform a 0-RTT AKE via a relayed server)

Cryptography Engineering

- Symmetric-key primitives
- MitM, Signature (ECDSA), Certificate, Reuse attack on DSA
- Signed Diffie-Hellman Key Exchange, TLS handshake, “Everything-over-TLS”
- Secure Messaging, X3DH (allows two users perform a 0-RTT AKE via a relayed server)

Cryptography Engineering

- Symmetric-key primitives
- MitM, Signature (ECDSA), Certificate, Reuse attack on DSA
- Signed Diffie-Hellman Key Exchange, TLS handshake, “Everything-over-TLS”
- Secure Messaging, X3DH
- Double Ratchet = Symmetric-key Ratchet + Diffie-Hellman Ratchet
  - Use Initial shared secret from X3DH to do secure messaging
  - Ensure forward secrecy and backward secrecy

Cryptography Engineering

- Symmetric-key primitives
- MitM, Signature (ECDSA), Certificate, Reuse attack on DSA
- Signed Diffie-Hellman Key Exchange, TLS handshake, “Everything-over-TLS”
- Secure Messaging, X3DH
- Double Ratchet = Symmetric-key Ratchet + Diffie-Hellman Ratchet
- Password-based Protocols:
  - Offline/Online dictionary attacks, precomputation (or rainbow-table) attack
  - Salted hash of passwords, add iteration (SCRAM)
  - OPAQUE: OPRF + AKE => PAKE that against precomputation attack

Cryptography Engineering

- Symmetric-key primitives
- MitM, Signature (ECDSA), Certificate, Reuse attack on DSA
- Signed Diffie-Hellman Key Exchange, TLS handshake, “Everything-over-TLS”
- Secure Messaging, X3DH
- Double Ratchet = Symmetric-key Ratchet + Diffie-Hellman Ratchet
- Password-based Protocols
- Attacks: Reuse attacks (salt, randomness), Downgrade attacks, Invalid inputs, …

Cryptography Engineering

- Symmetric-key primitives
- MitM, Signature (ECDSA), Certificate, Reuse attack on DSA
- Signed Diffie-Hellman Key Exchange, TLS handshake, “Everything-over-TLS”
- Secure Messaging, X3DH
- Double Ratchet = Symmetric-key Ratchet + Diffie-Hellman Ratchet
- Password-based Protocols
- Attacks
- Post-quantum Cryptography
  - Lattice-based, Isogeny-based, hash-based, code-based…
  - Crystals-Kyber (KEM), Crystals-Dilithium (Signature)
  - Hybrid Cryptography (TLS 1.3 + pqKEM), PQTLS (Kyber + Dilithium), KEM-TLS

Cryptography Engineering

- Symmetric-key primitives
- MitM, Signature (ECDSA), Certificate, Reuse attack on DSA
- Signed Diffie-Hellman Key Exchange, TLS handshake, “Everything-over-TLS”
- Secure Messaging, X3DH
- Double Ratchet = Symmetric-key Ratchet + Diffie-Hellman Ratchet
- Password-based Protocols
- Attacks
- Post-quantum Cryptography

Homework

- Homework:
  - DDL for homework set 3 and all bonus homework: **Feb 16th (Before next Monday)**
  - 1 non-bonus homework question = 1 point
  - 1 bonus homework question = 2 points

  - How to calculate the final grade of homework (≤ 40):

$$40 \times \left({}^{\text{points you obtain}} / _{\text{the number of questions}} \right)$$

// You need to get at least 40 × 60% = **24 points to qualify for the final exam**.

Final Project and Exam

- Final Project (Code + Report)
  - DDL: **March 7, 2025, at 23:59**
  - How to submit: **Send me via email**
  - The description (What to do, criteria of evaluation, etc…) of Final Project topic is in Moodle
  - Note: Post-quantum security is not necessary, but if you have…

- Exam:
  - When: **March 24, 2025**
  - Where: **Professor Pan's office (will notify again via Moodle)**