Norwegian University of Science and Technology

Teaching Cryptography at NTNU

Tjerand Silde on May 29, 2025

@Universidad Carlos III de Madrid

Faculty of Information Technology and Electrical Engineering at NTNU

- Department of Computer Science
- Department of Electric Energy
- Department of Electronic Systems
- Department of Engineering Cybernetics
- Department of ICT and Natural Sciences
- Department of Information Security and Communication Technology
- Department of Mathematical Sciences

Faculty of Information Technology and Electrical Engineering at NTNU

- Department of Computer Science
- Department of Electric Energy
- Department of Electronic Systems
- Department of Engineering Cybernetics
- Department of ICT and Natural Sciences
- **Department of Information Security and Communication Technology**
- **Department of Mathematical Sciences**

NTNU Applied Cryptology Lab

NTNU Applied Cryptology Lab

Study Programs with Cryptography

Cyber Security and Data Communication (5 years)

- Cryptographic Engineering profile

Digital Infrastructure and Cyber Security (2 years)

- (Two compulsory courses)

Master of Mathematical Sciences (2 years)

- Applied Algebra profile

Cryptography Courses

- TTM4135 Applied Cryptography and Network Security

- TTM4138 Wireless Network Security
- TTM4195 Blockchain Technologies and Cryptocurrencies
- TTM4205 Secure Cryptographic Implementations
- IMT4217 Introduction to Data Privacy
- TMA4160 Cryptography
- TMA4162 Computational Algebra

Secure Cryptographic Implementations

The course covers how to implement, analyse, attack, protect and securely compose cryptographic algorithms in practice.

It goes in depth on how to implement computer arithmetic, attacking implementations using side-channel attacks and fault injection, exploit padding oracles and low-entropy randomness, utilise techniques to defend against these attacks, and how to securely design misuse-resistant APIs.

Secure Cryptographic Implementations

- The course content is covered by the lecture slides and three different assignments as a portfolio

- Recommended literature:
  - Serious Cryptography by Jean-Philippe Aumasson
  - Real-World Cryptography by David Wong
  - The Hardware Hacking Handbook by Jasper van Woudenberg and Colin O'Flynn

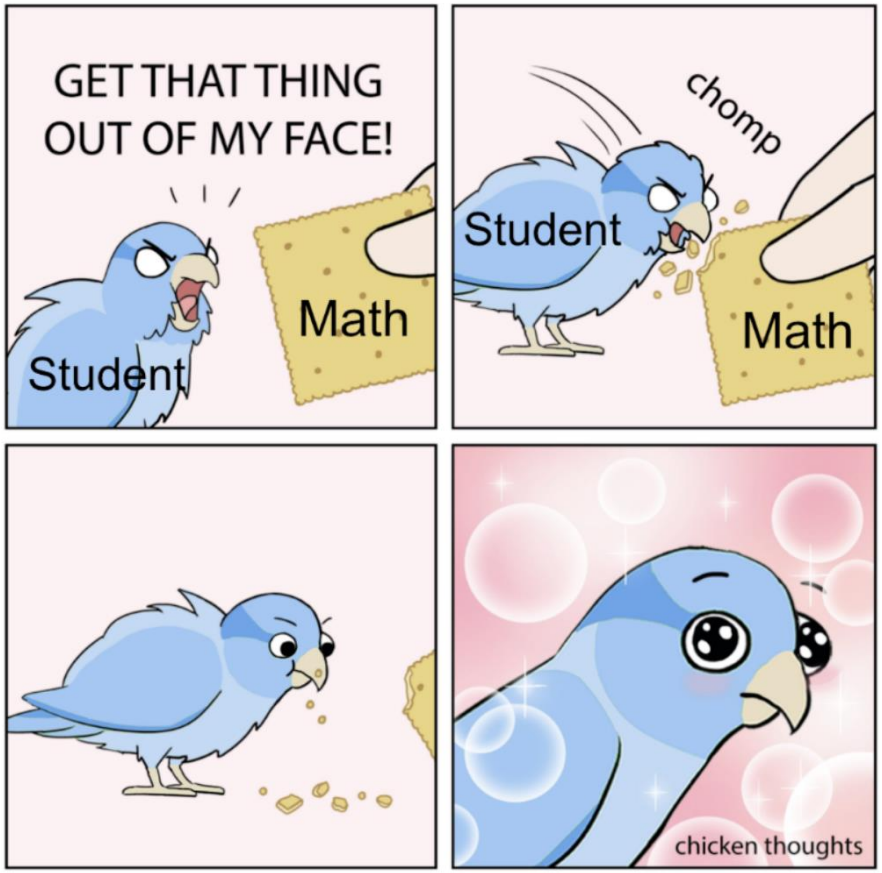
- We have 6 hours of lectures, lab, and exercise class per week

Secure Cryptographic Implementations

- Lecture topics:
  - Randomness
  - Legacy Cryptography
  - Post-Quantum Crypto
  - Padding Oracles
  - Side-Channel Attacks
  - Crypto API Failures
  - Commitments and ZKP
  - Protocol Composition
- Assignments:
  - Weekly problems (40%)
  - ChipWhisperer lab (20%)
  - Technical Essay (40%)
- All technical essays are presented in class
- Invited guest lectures

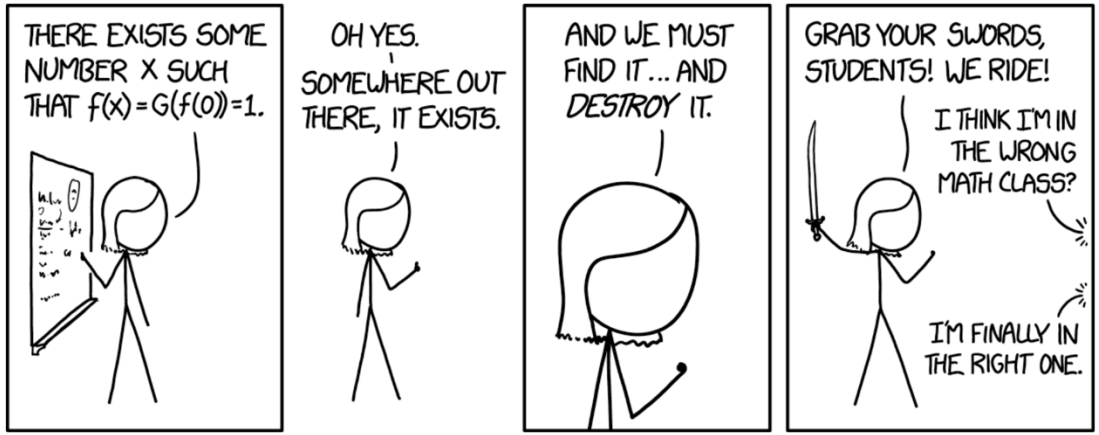
Secure Cryptographic Implementations

- It is a clear mix of mathematics and computer science
- We spend ~30% of the time on discussions
- All assignments are announced in August with a deadline in December



Secure Cryptographic Implementations

- Weekly problems:
  - Mathematics
  - Coding
  - CryptoHack



Secure Cryptographic Implementations

1.1 "It is truly random, I promise!"

Intel published a cryptography library with the following C++ code snippet:

```
1       static void rand32u(std::vector<Ipp32u>& addr) {
2               std::random_device dev;
3               std::mt19937 rng(dev());
4               std::uniform_int_distribution<std::mt19937::
                    ↪ result_type> dist(0, UINT_MAX);
5               for (auto& x : addr) x = (dist(rng) << 16) +
                    ↪ dist(rng);
6       }
```

Question 1: Give a high-level explanation of each line of code.

Question 2: This code was used to generate cryptographic keys, which are supposed to be of 128 bits entropy. However, there are two *catastrophic failures* in this snippet. What is wrong?

Question 3: Describe (in words and/or pseudocode) how to fix this.

Secure Cryptographic Implementations

4.2 Faulty RSA Bites the Dust

Let (n, e) be a public RSA signature verification key and (n, e') a public RSA encryption key for the same user, where $n = p \cdot q$ for secret prime numbers p, q and corresponding secret signing key d and decryption key d'.

Assume that the signing API Sign is implemented in a faulty way so that the signing key d leaks to malicious clients.

Question 1: How can the knowledge of the signing key d be used to decrypt messages encrypted using the public encryption key (n, e')?

Assume now that the leakage in Sign be fixed so that d is stored securely. Let μ be a secure padding function. The RSA signature is often computed using the Chinese Reminder Theorem in the following way:

1. Compute $d_p \equiv d \mod (p-1)$ and $d_q \equiv d \mod (q-1)$.
2. Compute a such that $a \equiv 1 \mod p$ and $a \equiv 0 \mod q$.
3. Compute b such that $b \equiv 0 \mod p$ and $b \equiv 1 \mod q$.
4. Compute $\sigma_p \equiv \mu(m)^{d_p} \mod p$ and $\sigma_q \equiv \mu(m)^{d_q} \mod q$.
5. Output the signature $\sigma = a \cdot \sigma_p + b \cdot \sigma_q \mod n$.

This is more efficient than computing $\mu(m)^d \mod n$ directly since p and q are much smaller than n and (d_p, d_q, a, b) can be pre-computed and stored for later use. We can verify the signature as following: $\mu(m) \stackrel{?}{\equiv} \sigma^e \mod n$.

Question 2: Assume that there is a bug in the implementation so that $\sigma_p \equiv \mu(m)^{d_p} \mod p$ but $\sigma_q \not\equiv \mu(m)^{d_q} \mod q$. Show how the faulty signature σ, where $\mu(m) \not\equiv \sigma^e \mod n$, can be used to factor n.

Secure Cryptographic Implementations

- ChipWhisperer lab:
  - AES, RSA, and ECC
  - Four weeks of lab
  - Written report

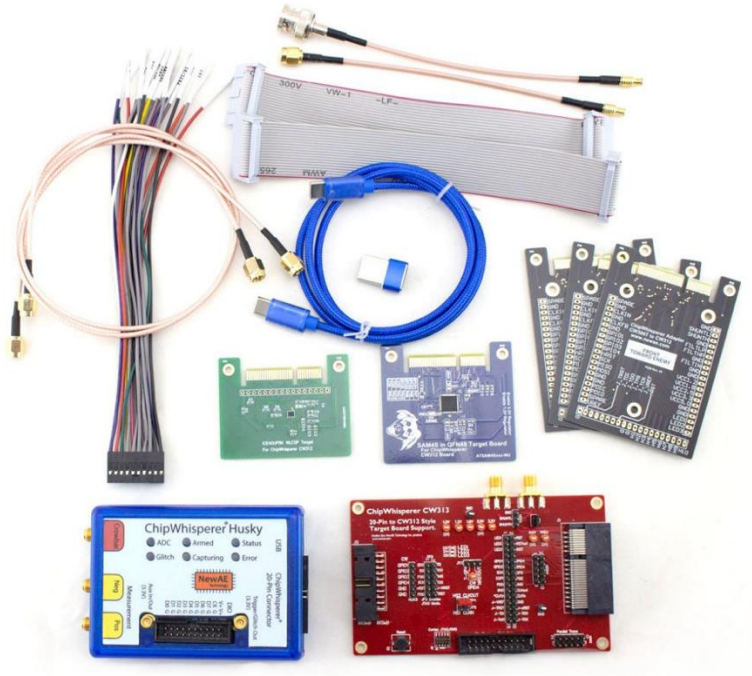
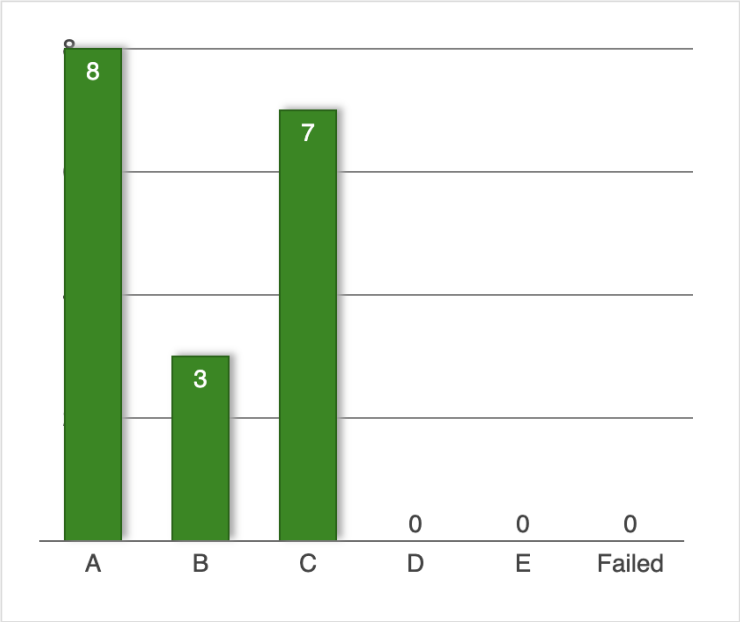


Figure: ChipWhisperer Husky

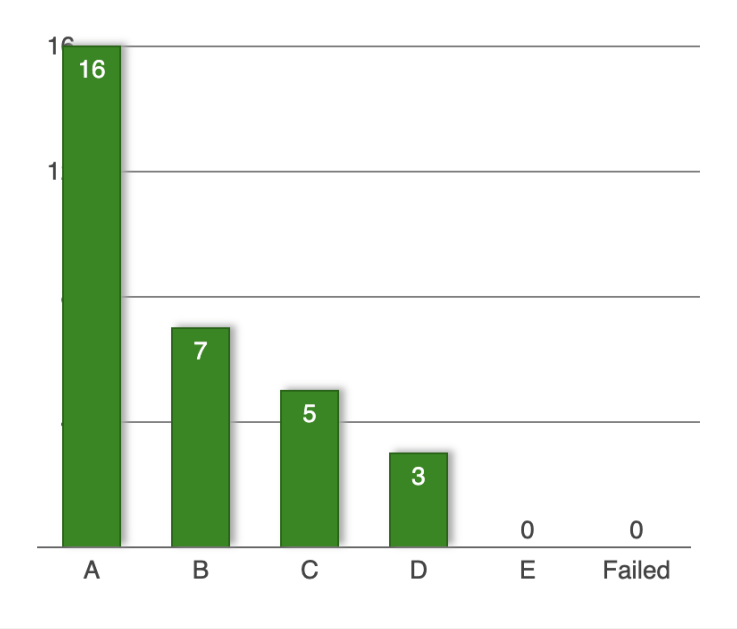
Secure Cryptographic Implementations

- Technical essay:
  - 2-3 students per group
  - 8-10 page essay
  - They suggest topics

Secure Cryptographic Implementations



Average grade: B



Average grade: B

Secure Cryptographic Implementations

- Students are generally active and appreciate the course
- It requires a lot of work throughout the whole semester
- I have students from several different study programs
- It is also quite popular among international students
- All of my materials are available at ttm4205.iik.ntnu.no

Norwegian University of
Science and Technology

THANKS!