# Quantum Cryptography and Quantum Key Distribution Notes

Gergely Lendvay

February 5, 2026

# Contents

0.1 Course Info . . . . . 4

0.1.1 Teachers . . . . . 4

0.1.2 Exercise Classes . . . . . 4

0.1.3 Exam . . . . . 4

0.1.4 Books . . . . . 4

0.2 Plan . . . . . 4

**1 First Lecture 5**

1.1 Classical Cryptography . . . . . 5

1.2 RSA Encryption Scheme . . . . . 5

**2 Second Lecture 8**

2.1 Provably Secure Cryptography . . . . . 8

2.2 Quantum Key Distribution . . . . . 9

**3 Third Lecture 9**

# List of Acronyms

| | |
|---|---|
| AES | Advanced Encryption Standard |
| RSA | Rivest–Shamir–Adleman |
| PQC | Post-Quantum Cryptography |
| QKD | Quantum Key Distribution |

# Introduction

## 0.1 Course Info

### 0.1.1 Teachers

Konstantin Wernli – kwernli@imada.sdu.dk
William Mistegard – wem@imada.sdu.dk
Jurek Bleischwitz – jurek@imada.sdu.dk

### 0.1.2 Exercise Classes

1. Solutions must be uploaded before each class.
2. Exercise sheets are discussed during the classes.
3. The four best exercise solutions count towards the overall course grade.

### 0.1.3 Exam

1. Assessment is based on four graded exercise sheets, and
2. Final oral exam consisting of:
    - 10–12 minutes presentation,
    - 13–15 minutes discussion and questions,
    - 5 possible topics, with 30 minutes of preparation time.
3. Tentative exam date: June 9, 2026

### 0.1.4 Books

Quantum Key Distribution – Ramona Wolf

## 0.2 Plan

The course begins with an introduction to classical cryptography and quantum key distribution (QKD), followed by a recap of quantum computing and quantum information theory. Subsequent topics include post-processing, security analysis, practical implementations of QKD, and post-quantum cryptography.

# 1 First Lecture

## 1.1 Classical Cryptography

The fundamental problem of cryptography is to enable secure communication between two parties, traditionally called Alice and Bob, while preventing an adversary Eve from gaining any information about the transmitted message.

Classical cryptography includes examples, such as the Caesar cipher, while more modern schemes can be categorized either by symmetric or asymmetric schemes. Well-known examples include Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman (RSA).

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Plain Alphabet** | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| **Cipher Alphabet** | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |

Table 1: Caesar Cipher Table (Right Shift by 3)

**Impact of Quantum Computing on Classical Cryptography** One of the major implications of quantum computing is its ability to efficiently solve certain mathematical problems that are believed to be hard for classical computers. In particular, efficient prime factorization through Shor's algorithm would render widely used public-key cryptographic schemes such as RSA insecure.

## 1.2 RSA Encryption Scheme

The RSA algorithm was introduced in 1977 by Rivest, Shamir, and Adleman and is still widely used, making up approximately 50% of all asymmetric encryption schemes. The goal is to find 3 integers $n$, $e$, and $d$ such that for all messages

$$x \in \{0, \ldots, n-1\},$$

the following holds:

$$(x^e)^d \equiv x \pmod{n}.$$

**Key Generation** Two large random prime numbers $p$ and $q$ are chosen, typically satisfying

$$2^{1023} < p, q < 2^{1024}.$$

The public modulus is defined as

$$n = pq.$$

Let $\lambda(n)$ denote Carmichael's function,

$$\lambda(n) = \mathrm{km}(p-1, q-1).$$

An integer $e$ is chosen such that

$$1 < e < \lambda(n), \qquad \gcd(e, \lambda(n)) = 1.$$

The private key $d$ is defined as the modular inverse of $e$ modulo $\lambda(n)$:

$$d \equiv e^{-1} \pmod{\lambda(n)}.$$

**Encryption and Decryption** The public key $(n, e)$ is made available to everyone, while the private key $d$ is kept secret. To send a message $x$, Bob computes the ciphertext

$$y \equiv x^e \pmod{n}$$

and sends $y$ to Alice. Using her private key, Alice decrypts the message by computing

$$y^d = (x^e)^d \equiv x \pmod{n}.$$

An eavesdropper Eve, even knowing $n$, $e$, and the encrypted message $y$, cannot efficiently recover $x$ without access to $d$. This is because computing $d$ requires knowledge of $\lambda(n)$, which in turn requires factoring $n$ into $p$ and $q$.

**Proof** Since $n = pq$,

$$m^{ed} \equiv m \pmod{p} \quad \text{and} \quad m^{ed} \equiv m \pmod{q}.$$

Because

$$ed \equiv 1 \pmod{\lambda(n)},$$

there exists an integer $k$ such that

$$ed - 1 = k(p-1).$$

Then, for $x \not\equiv 0 \pmod{p}$,

$$m^{ed-1} = m^{k(p-1)} = (m^{p-1})^k = 1^k \equiv 1 \pmod{p},$$

by Fermat's Theorem, which states that if $p$ is a prime and $\gcd(m, p) = 1$, then

$$m^{p-1} \equiv 1 \pmod{p}.$$

The same argument holds for $q$.

**Security Assumptions** The security of RSA relies on the computational hardness of factoring large integers. The best known classical factoring algorithms run in sub-exponential time,

$$\exp(c(\log n)^{1/3}(\log \log n)^{2/3}),$$

which is infeasible for sufficiently large $n$.

**Quantum Threat** Shor's algorithm shows that a quantum computer can factor integers in polynomial time,

$$O((\log n)^3).$$

This would completely break RSA if large-scale, fault-tolerant quantum computers become available.

Currently, practical limitations such as qubit count, noise, and error correction prevent Shor's algorithm from being applied. In practice, breaking RSA would require millions of qubits.

Even if RSA remains secure in the near term, cryptographic systems must be developed that are resistant to quantum attacks. This includes both new classical schemes (post-quantum cryptography) and quantum approaches such as Quantum Key Distribution (QKD).

# 2 Second Lecture

## 2.1 Provably Secure Cryptography

Example: RSA is not proven to be secure against a polynomial adversary as it can be broken with an infinitely good computer.

An encryption scheme is secure if we can mathematically prove it.

Example: One-time pad (Vernam cipher, 1926): Alice and Bob share a secret key $S_A = S_B \in \{0,1\}^*$ without Eve knowing. Alice encrypts the message $m \in \{0,1\}^*(c)_i = m_i \oplus (S_A)_i$

$$S_A = 101, \qquad m = 011, \qquad c = 110$$

Alice then sends the encrypted message $c$ to Bob and decrypts it: $m'_i = c_i \oplus (S_B)_i$

$$m'_i = c_i \oplus (S_B)_i = (m_i \oplus (S_A)_i) \oplus (S_B)_i = m_i \oplus ((S_A)_i \oplus (S_B)_i) = m_i \oplus 0 = m_i$$

One can prove that $c$ provides no information about $m$ given that:

1. Key must be random
2. Key is as long as the message
3. Key is not re-used
4. Key must be completely secret

mathematical properties of the key: Ideally:

1. Correctness $S_A = S_B$
2. Randomness $P[S = S] = 2^{-n}$
3. Eve has no information about the key

More realistically: $P[S_A \neq S_B] < \epsilon$ Close to uniformly random, individual bits are independent If Eve interferes with key generation, then we do not produce a key

## 2.2 Quantum Key Distribution

BB84, Bennett Brassard 1984

Eve can listen to the classical channel, with complete access to the quantum channel

**Quantum Transmission** Alice chooses two bit-strings at random: $a, b \in \{0,1\}^*$ where $a$ is the key and $b$ is the encoding basis.

Alice prepares qubit states $|\psi_i\rangle$ by encoding $a_i$:

1. In the computational basis, $|0\rangle$ and $|1\rangle$
2. Diagonal basis $|+\rangle$, $|-\rangle$

Alice sends them across the quantum channel

Bob chooses $b'$ at random and measures $|\psi_i\rangle$ in basis $b_i$: $a_i' =$ measurement of $|\psi_i\rangle$ in basis $b_i'$ If $b_i' = b_i$ then $a_i' = a_i$ else if $b_i' \neq b_i$ then $a_i'$ is uniformly random and gets discarded

If $b_i' = b_i$: $0 \to |0\rangle, 1 \to |1\rangle$, then in a computational basis state, $P_\psi(0) = |\langle 0| |\psi\rangle|^2$ and $P_\psi(1) = |\langle 1| |\psi\rangle|^2$ $P_{|0\rangle}(0) = 1$ and $P_{|0\rangle}(1) = 0$, meaning $a_i' = 0$

if $b_i' \neq b_i$, then $a_i = 0$ $a_i = 0, b_i = 1 \to |\psi_i\rangle = |+\rangle$ $P_{|+\rangle}(0) = \frac{1}{2} and P_{|+\rangle}(1) = \frac{1}{2}$

Alice and Bob compare $b$ and $b'$ and discard $a_i$ for all $i$ where $b_i \neq b_i'$, where for the remaining $a_i = a_i'$

No cloning theorem prevents Eve from learning the quantum states Alice send Bob

# 3 Third Lecture