

# Introduction

How all the pieces fit together

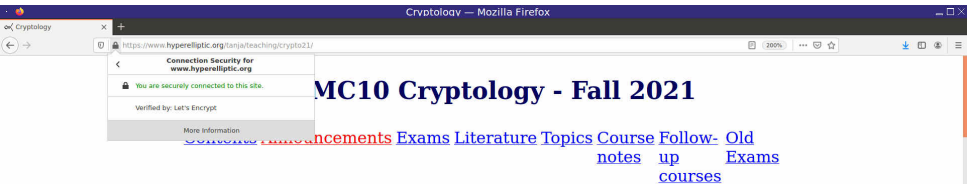
Tanja Lange

Eindhoven University of Technology

2MMC10 – Cryptology

# Cryptology page

<https://www.hyperelliptic.org/tanja/teaching/crypto21/>



The screenshot shows a Mozilla Firefox browser window with the address bar displaying <https://www.hyperelliptic.org/tanja/teaching/crypto21/>. A connection security warning is visible, stating "Connection Security for www.hyperelliptic.org" and "You are securely connected to this site." Below the warning, there are navigation links: "MC10 Cryptology - Fall 2021", "Announcements", "Exams", "Literature", "Topics", "Course", "Follow-up", "Old Exams", and "courses".

[Tanja Lange](#)

[Coding Theory and Cryptology](#)

[Eindhoven Institute for the Protection of Information](#)

[Department of Mathematics and Computer Science](#)

Room MF 6.104B

[Technische Universiteit Eindhoven](#)

P.O. Box 513

5600 MB Eindhoven

Netherlands

Phone: +31 (0) 40 247 4764

The easiest ways to reach me wherever I am:

e-mail: [tanja@hyperelliptic.org](mailto:tanja@hyperelliptic.org)

- This page belongs to course 2MMC10 - Cryptology. This course is offered at TU/e and aimed at students of mathematics and computer science.

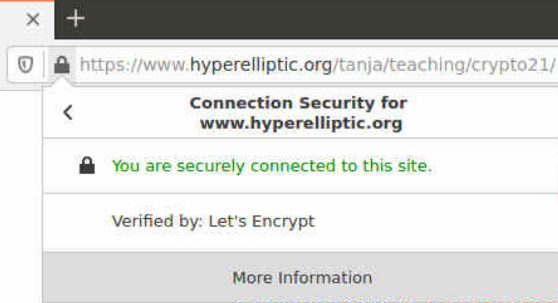
## Contents

- The general structure of block ciphers, Feistel ciphers like DES, AES, the most suitable modes-of-use, e.g. CBC or GCM

# Cryptology page

<https://www.hyperelliptic.org/tanja/teaching/crypto21/>

Cryptolo



MC10 Cry

[Certificates](#) [Announcements](#) [Exams](#)

[Lange](#)

g Theory and Cryptology

# Cryptology page

<https://www.hyperelliptic.org/tanja/teaching/crypto21/>

Page Info — <https://hyperelliptic.org/tanja/news.html>



## Website Identity

Website: hyperelliptic.org

Owner: This website does not supply ownership information.

Verified by: Let's Encrypt

[View Certificate](#)

Expires on: November 8, 2021

## Privacy & History

Have I visited this website prior to today?

Yes, 9 times

Is this website storing information on my computer?

No

[Clear Cookies and Site Data](#)

Have I saved any passwords for this website?

No

[View Saved Passwords](#)

## Technical Details

Connection Encrypted (TLS\_AES\_256\_GCM\_SHA384, 256 bit keys, TLS 1.3)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

[Help](#)

# More details

<https://www.ssllabs.com/ssltest/analyze.html?d=hyperelliptic.org>

SSL Server Test: hyperelliptic.org (Powered by Qualys SSL Labs) — Mozilla Firefox

https://www.ssllabs.com/ssltest/analyze.html?d=hyperelliptic.org

200%

...

...

## Cipher Suites

### # TLS 1.3 (suites in server-preferred order)

TLS\_AES\_256\_GCM\_SHA384 (0x1302) ECDH x25519 (eq. 3072 bits RSA) FS

TLS\_CHACHA20\_POLY1305\_SHA256 (0x1303) ECDH x25519 (eq. 3072 bits RSA) FS

TLS\_AES\_128\_GCM\_SHA256 (0x1301) ECDH x25519 (eq. 3072 bits RSA) FS

### # TLS 1.2 (suites in server-preferred order)

TLS\_ECDHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256 (0xcc8) ECDH x25519 (eq. 3072 bits RSA) FS

TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc030) ECDH x25519 (eq. 3072 bits RSA) FS

TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 (0xc028) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**

TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02f) ECDH x25519 (eq. 3072 bits RSA) FS

TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (0xc027) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**

TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0x9f) DH 2048 bits FS

TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256 (0x6b) DH 2048 bits FS **WEAK**

TLS\_ECDHE\_RSA\_WITH\_ARIA\_256\_GCM\_SHA384 (0xc061) ECDH x25519 (eq. 3072 bits RSA) FS

TLS\_ECDHE\_RSA\_WITH\_ARIA\_128\_GCM\_SHA256 (0xc060) ECDH x25519 (eq. 3072 bits RSA) FS

TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (0xc014) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**

## Understand what this means

- How can it be that I talk to the server securely?  
Why do we have have a shared secret without ever meeting?
- How do I know that I talk to the correct server?
- How do I receive or send data secure?
- How is this data secured against modification?

## Understand what this means

- How can it be that I talk to the server securely?  
Why do we have have a shared secret without ever meeting?
- How do I know that I talk to the correct server?
- How do I receive or send data secure?
- How is this data secured against modification?

### Important distinction

#### **Public-key cryptography**

Each user has 2 keys:  
a public key and a private key.

Public key can be posted online;  
private key must be kept secret.

Often can compute public key  
from private key.  
Other direction must be hard.

#### **Symmetric-key cryptography**

Each pair of users shares a key.  
Knowledge of this key is symmetric  
between both.

This key must be kept secret.

Symmetric systems often faster  
than public-key systems.  
Use latter to get symmetric key.

## Understand what this means

- How can it be that I talk to the server securely?
- Why do we have have a shared secret without ever meeting?
- How do I know that I talk to the correct server?
- How do I receive or send data secure?
- How is this data secured against modification?

### Important distinction

#### Public-key cryptography

Each user has 2 keys:  
a public key and a private key.

Public key can be posted online;  
private key must be kept secret.

Often can compute public key  
from private key.  
Other direction must be hard.

#### Symmetric-key cryptography

Each pair of users shares a key.  
Knowledge of this key is symmetric  
between both.

This key must be kept secret.

Symmetric systems often faster  
than public-key systems.  
Use latter to get symmetric key.



## Understand what this means

- How can it be that I talk to the server securely?  
Why do we have have a shared secret without ever meeting?
- How do I know that I talk to the correct server?
- How do I receive or send data secure?
- How is this data secured against modification?

### Important distinction

#### Public-key cryptography

Each user has 2 keys:  
a public key and a private key.

Public key can be posted online;  
private key must be kept secret.

Often can compute public key  
from private key.  
Other direction must be hard.

#### Symmetric-key cryptography

Each pair of users shares a key.  
Knowledge of this key is symmetric  
between both.

This key must be kept secret.

Symmetric systems often faster  
than public-key systems.  
Use latter to get symmetric key.