Cryptography and Network Security

Mario Cagalj

University of Split

Administrative Information

Course Webpage

https://cns.mario-cagalj.from.hr

- Lecture presentations
- Course description, laboratory exercises, literature
- Links to online books and other interesting references
- Various announcements (+ Moodle)

Evaluation Criteria and Grading

The final grade is formed approximately as follows:

Exam 1 (midterm 1)	40%
Exam 2 (midterm 2)	50%
Labs	10%

Hands-on Labs

- Earning points by solving cryptography challenges
- Challenges provided via REST API server (Pyton FastAPI)
- Students submit solutions (including source code) via a local GitLab server

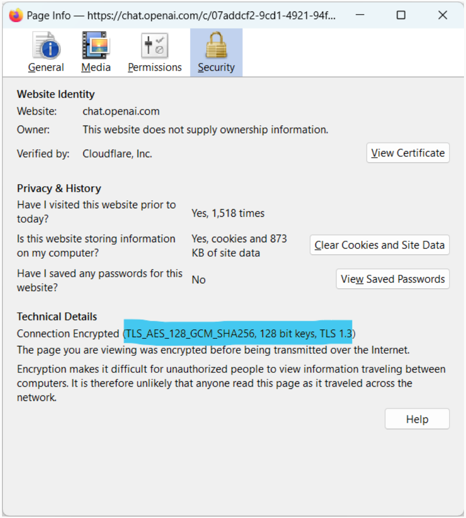
`https://github.com/mcagalj/CNS-2023-24`

Course Content Overview

- Symmetric and asymmetric cryptography
- Encryption modes
- Authenticated encryption schemes
- Authentication functions
- Digital signatures, message authentication codes
- Network security protocols (TLS and SSH)
- Web security (HTTPS, auth tokens, passkeys)
- WiFi security (if time permits)

Real-World Cryptography

Real-World Cryptography



Page Info — https://chat.openai.com/c/07addcf2-9cd1-4921-94f...

Website Identity

Website: chat.openai.com

Owner: This website does not supply ownership information.

Verified by: Cloudflare, Inc.

Privacy & History

Have I visited this website prior to today?	Yes, 1,518 times	
Is this website storing information on my computer?	Yes, cookies and 873 KB of site data	Clear Cookies and Site Data
Have I saved any passwords for this website?	No	View Saved Passwords

Technical Details

Connection Encrypted (TLS_AES_128_GCM_SHA256, 128 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.

Real-World Cryptography

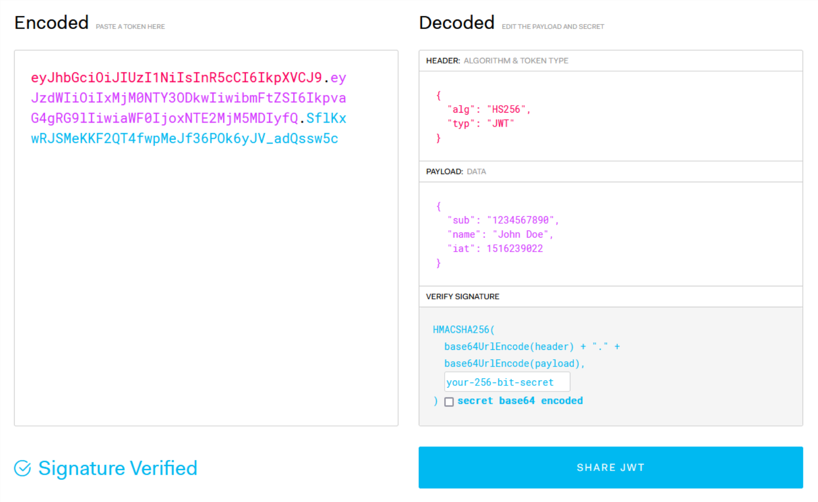
```
ssl_protocols TLSv1.2 TLSv1.3;
ssl_prefer_server_ciphers off;
ssl_ciphers "ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-...";

server {
    server_name cns.mario-cagalj.from.hr;

    ...

    ssl_certificate /etc/letsencrypt/live/.../fullchain.pem;
    ssl_certificate_key /etc/letsencrypt/live/.../privkey.pem;
    include /etc/letsencrypt/options-ssl-nginx.conf;
    ssl_dhparam /etc/letsencrypt/ssl-dhparams.pem;
}
```

Real-World Cryptography



Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.ey
JzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6Ikpva
G4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKx
wRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

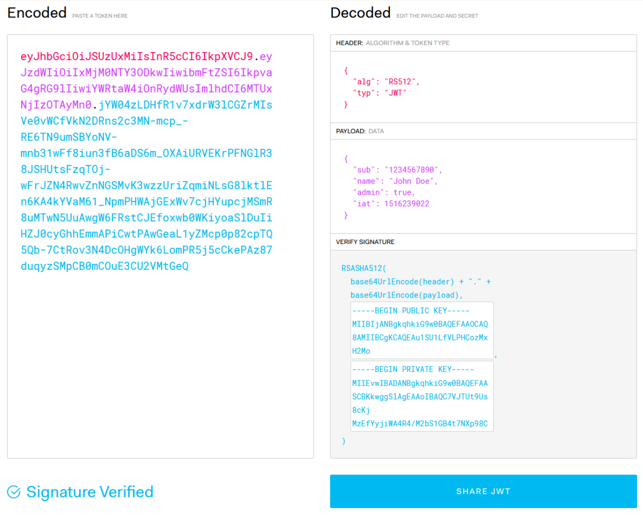
```
{
  "sub": "1234567890",
  "name": "John Doe",
  "iat": 1516239022
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) □ secret base64 encoded
```

Signature Verified

Real-World Cryptography



Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJSUzUxMiIsInR5cCI6IkpXVCJ9.ey
JzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6Ikpva
G4gRG9lIiwiYWRtaW4iOnRydWUsImlhdCI6MTUx
NjIzOTAyMn0.jYW04zLDHfR1v7xdrW31CGZrMIs
Ve0vWCfVkN2DRns2c3MN-mcp_-
RE6TN9umSBYoNV-
mnb31wFf8iun3fB6aDS6m_OXAiURVEKrPFNGlR3
8JSHUtsFzqTOj-
wFrJZN4RwvZnNGSMvK3wzzUriZqmiNLsG8lktlE
n6KA4kYVaM61_NpmPHWAjGExWv7cjHYupcjMSmR
8uMTwN5UuAwgW6FRstCJEfoxwb0WKiyoaSlDuIi
HZJ0cyGhhEmmAPiCwtPAwGeaL1yZMcp0p82cpTQ
5Qb-7CtRov3N4DcOHgWYk6LomPR5j5cCkePAz87
duqyzSMpCB0mCOuE3CU2VMtGeQ
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "RS512",
  "typ": "JWT"
}
```

PAYLOAD: DATA

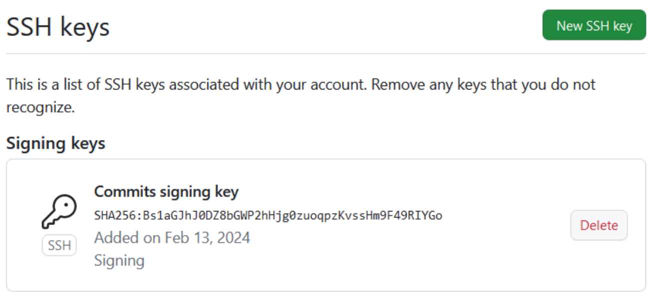
```
{
  "sub": "1234567890",
  "name": "John Doe",
  "admin": true,
  "iat": 1516239022
}
```

VERIFY SIGNATURE

```
RSASHA512(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  -----BEGIN PUBLIC KEY-----
  MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ
  8AMIIBCgKCAQEAu1SU1LfVLPHCozMx
  H2Mo
  ,
  -----BEGIN PRIVATE KEY-----
  MIIEvwIBADANBgkqhkiG9w0BAQEFAA
  SCBKkwggSlAgEAAoIBAQC7VJTUt9Us
  8cKj
  MzEfYyjiWA4R4/M2bS1GB4t7NXp98C
)
```

✓ Signature Verified

Real-World Cryptography



SSH keys

This is a list of SSH keys associated with your account. Remove any keys that you do not recognize.

Signing keys

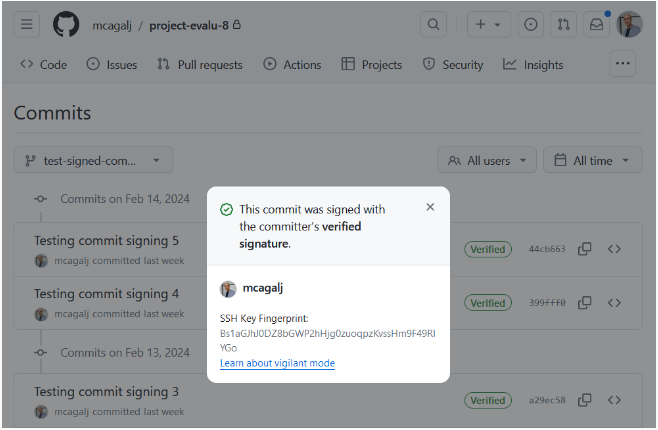
Commits signing key

SHA256:Bs1aGJhJ0DZ8bGWP2hHjg0zuoqpzKvssHm9F49RIYGo

Added on Feb 13, 2024

Signing

Real-World Cryptography



Commits

Commits on Feb 14, 2024

Testing commit signing 5
mcagalj committed last week
Verified 44cb663

Testing commit signing 4
mcagalj committed last week
Verified 399fff0

Commits on Feb 13, 2024

Testing commit signing 3
mcagalj committed last week
Verified a29ec58

This commit was signed with the committer's **verified signature**.

mcagalj

SSH Key Fingerprint:
Bs1aGJhJ0DZ8bGWP2hHjg0zuoqpzKvssHm9F49RIYGo

Learn about vigilant mode

Real-World Cryptography

Git protocol uses a hash function for content-based naming and to organize content into an efficient Merkle tree.

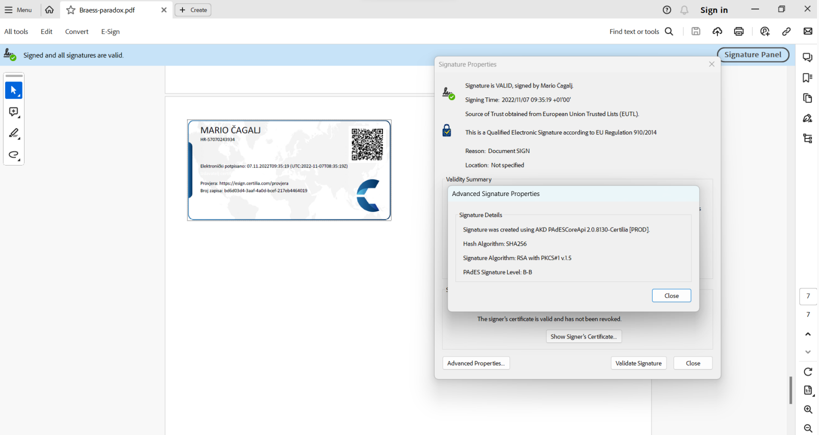
```
$ git cat-file -p 71e42b1e10424661104dff8b174784706fa3203e

040000 tree b1db1748961ceae6c81e446154546ac419551971    certificates
040000 tree 7f0746313766a9738b4e5b0f49cde84dd226841e    migrations
100644 blob b208bbb8550f1447d5fbcaea6c3a823d8718620e    schema.prisma
```

```
$ git hash-object -w schema.prisma

b208bbb8550f1447d5fbcaea6c3a823d8718620e
```

Real-World Cryptography



Signed and all signatures are valid.

MARIO ČAGALJ
HR-57070243934

Elektronički potpisano: 07.11.2022T09:35:19 (UTC:2022-11-07T08:35:19Z)

Provjera: https://esign.certilia.com/provjera
Broj zapisa: bd6d03d4-3aaf-4a0d-bcef-217eb4464019

Signature Properties

Signature is VALID, signed by Mario Čagalj.

Signing Time: 2022/11/07 09:35:19 +01'00'

Source of Trust obtained from European Union Trusted Lists (EUTL).

This is a Qualified Electronic Signature according to EU Regulation 910/2014

Reason: Document SIGN

Location: Not specified

Validity Summary

Advanced Signature Properties

Signature Details

Signature was created using AKD PAdESCoreApi 2.0.8130-Certilia [PROD].

Hash Algorithm: SHA256

Signature Algorithm: RSA with PKCS#1 v.1.5

PAdES Signature Level: B-B

Close

The signer's certificate is valid and has not been revoked.

Show Signer's Certificate...

Advanced Properties...

Validate Signature

Close

Real-World Cryptography

- Android Cryptography[1]
- Android Keystore

```
import android.security.keystore.KeyProperties
...
companion object {
    private const val ALGORITHM = KeyProperties.KEY_ALGORITHM_AES
    const val BLOCK_MODE_CBC = KeyProperties.BLOCK_MODE_CBC
    private const val PADDING = KeyProperties.ENCRYPTION_PADDING_PKCS7
    private const val KEY_SIZE = 256
    private const val CBC_CIPHER = "$ALGORITHM/$BLOCK_MODE_CBC/$PADDING"
    ...
}
```

[1] Click to follow hyperlink

Real-World Cryptography

WhatsApp's encryption system based on Signal protocol.

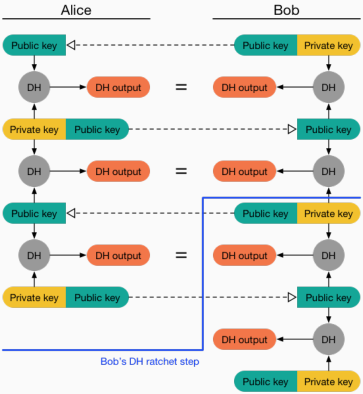
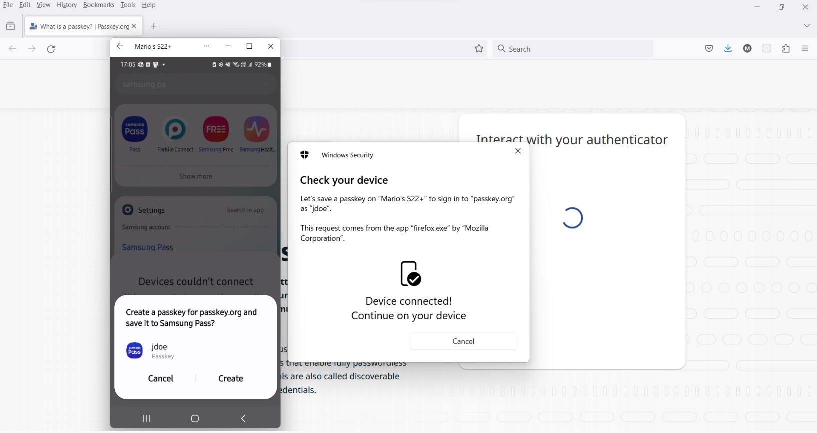


Figure 1: Double ratchet protocol: (source: signal.org)

Passkeys



Interact with your authenticator

Devices couldn't connect

Create a passkey for passkey.org and save it to Samsung Pass?

jdoe
Passkey

Check your device

Let's save a passkey on "Mario's S22+" to sign in to "passkey.org" as "jdoe".

This request comes from the app "firefox.exe" by "Mozilla Corporation".

Device connected!
Continue on your device

s that enable fully passwordless
ls are also called discoverable
edentials.

Real-World Cryptography

- Android Cryptography[2]
- Android Keystore

```
import android.security.keystore.KeyProperties
...
companion object {
    private const val ALGORITHM = KeyProperties.KEY_ALGORITHM_AES
    const val BLOCK_MODE_CBC = KeyProperties.BLOCK_MODE_CBC
    private const val PADDING = KeyProperties.ENCRYPTION_PADDING_PKCS7
    private const val KEY_SIZE = 256
    private const val CBC_CIPHER = "$ALGORITHM/$BLOCK_MODE_CBC/$PADDING"
    ...
}
```

[2] Click to follow hyperlink

Real-World Cryptography

- Storing passwords

  `$argon2id$v=19$m=65536,t=3,p=4$ZOL9wdqTOwsLo8tw3gW9Og$LjqqWI6g6Yey8...`
- Password managers[3]

[3] Click to follow hyperlink

Real-World Cryptography

(Cloud) Database encryption

- Transparent data encryption[4]
- Column-level encryption
- Field-level encryption

[4] Click to follow hyperlink

Real-World Cryptography

Google Cloud

- Encryption at rest[5]
- Encryption in transit
- Application layer transport security

[5] Click to follow hyperlink

Real-World Cryptography

Blockchain technology

- Cryptocurrency
- Web 3.0[6]
- Supply chain management

Related append-only ledgers/records

- Key transparency
- Certificate transparency

[6] Click to follow hyperlink

Real-World Cryptography

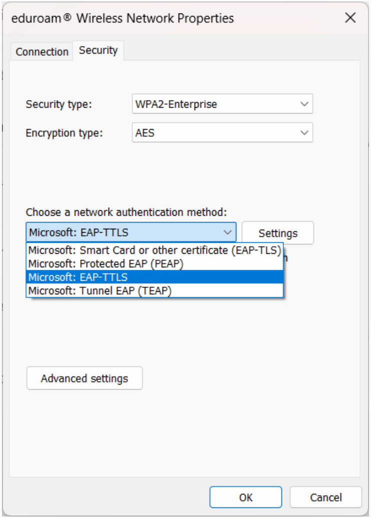
VPN

- OpenVPN (TLS-based)[7]
- strongSwan (IPsec-based)
- WireGuard

Related: MACsec

[7] Click to follow hyperlink

Real-World Cryptography



eduroam® Wireless Network Properties

Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method: Microsoft: EAP-TTLS

Connection
Security
Settings
Microsoft: Smart Card or other certificate (EAP-TLS)
Microsoft: Protected EAP (PEAP)
Microsoft: EAP-TTLS
Microsoft: Tunnel EAP (TEAP)
Advanced settings
OK
Cancel

Edward Snowden

Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on. Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it.