

Kryptographie

Laborprotokoll Übung 3



Figure 1: Wunderbares Gruppenbild

Unterrichtsgegenstand: ITSI|ZIVK
Jahrgang: 3AHITN
Name: Stefan Fürst, Marcel Raichle
Gruppenname/Nummer: Dumm und Dümmer/7
Betreuer: ZIVK
Übungsdaten: 24.5.2024, 31.5.2024, 7.6.2024
Abgabedatum: 7.6.2024

Contents

1	Aufgabenstellung	3
2	Zusammenfassung	3
3	Übungsdurchführung	4
3.1	Symmetrisch Verschlüsseln Übung 1	4
3.2	Asymmetrisch Verschlüsseln Übung 1	4
3.3	Integrität prüfen	4
4	Quellen	5
5	Abbildungsverzeichnis	6

1 Aufgabenstellung

2 Zusammenfassung

3 Übungsdurchführung

3.1 Symmetrisch Verschlüsseln Übung 1

zum verschlüsseln:

```
openssl aes256 -in Raichle.txt -out Raichle.encrypted
```

zum entschlüsseln

3.2 Asymmetrisch Verschlüsseln Übung 1

```
openssl aes256 -d -in Raichle.encrypted -out Raichle.txt Private key
```

```
openssl genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:4096 -out private-key.pem
```

```
openssl pkey -in private-key.pem -out public-key.pem -pubout
```

Pub key

```
datei verschlüsseln openssl rsautl -encrypt -inkey zivk.pem -pubin -in Raichle-Fuerst-RSA.txt -out Raichle-Fuerst-RSA.txt.zivk.enc
```

3.3 Integrität prüfen

command: `sha256sum <dateiname>` Hash erste datei e605bd1f525b133340d704f0e899d977f37dea63c14b243a346f1b524499bcf4te aus der liste 2. 591ad652f7332fdca28e4ecc520ad7b71852cdaa7ab3efbaeeb6042a815c812d 1te aus der liste 3. e05c11789a98a495d7283a499b1ccc31c368d3c191a4fb5b7074161c816da2e3 2te aus der liste 4. a20fb601802f7b87b2063964e0d2f5te aus der liste
der 3te hat keinen hash

4 Quellen

References

5 Abbildungsverzeichnis

List of Figures

1	Wunderbares Gruppenbild	1
---	-----------------------------------	---