COSIC

KU LEUVEN

H05E1A and H05D9A

Cryptography and Network Security 2023-2024

Prof. Bart Preneel

COSIC

Firstname.Lastname(at)esat.kuleuven.be

http://homes.esat.kuleuven.be/~preneel

September 2023

1

1

Kind request
Please register in your ISP

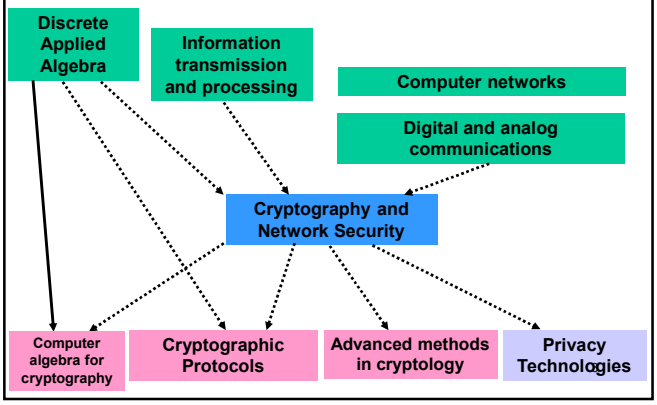
H05E1A Cryptography and Network Security

instead of

H05D9A Cryptografie en Netwerkbeveiliging

2

Relation to other courses



3

Related cryptography courses

Semester 1:

- Cryptography and Network Security (3): introduction and applications to payment and network security
- Cryptographic Protocols (4): focus on protocols and applications

Semester 2:

- Advanced Methods in Cryptography (4): focus on inner workings of algorithms and security proofs
- Computer Algebra for Cryptography (3): focus on computational tools

4

Related courses: privacy

Uses some cryptographic techniques but also other techniques

Semester 1:

- Privacy Technologies (3)
- Privacy and Big Data (4)

Semester 2:

- Advanced Privacy Technologies (4)

5

Other related courses

Semester 1:

- E-Security (3)

Semester 2:

- Hardware Security (3)

6

H05E1A and H05D9A Cryptography and Network Security

- Lectures on Thursday 10:35-12:30
- Tentative schedule (add two in October to end earlier?)
  - 28 September, 5-19 October (Aula ESAT L)
  - Extra: 3 October 10:35 and 16 October 16:05 (room TBC)
  - No lecture on 12, 26 October, 2 November
  - 9-16-23-30 November, 7 December (C300-00.77 aula E)
- Exercises: (10:35-13:00 default)
  - 6-7 November (ELEC B91.100/200)
  - 10 (16:05) - 13 November (ELEC B91.200/100)
  - 1 (16:05) - 4 December (ELEC B91.200)
  - For last session: eID card bring laptop
- Presentations: 20-21 December – extra slots may be added if needed (details to follow soon on Toledo)

7

H05E1A/H05D9A Cryptography and Network Security

- Course: Toledo – slides and general articles
  - I recommend that you attend/watch the lectures to understand the basic concepts
- Toledo: course, self-study, links, exercises, solutions,…
- 2 exercise sessions
- 1 practicum (eID/WiFi) (mandatory)
- **Install and use PGP or GPG (mandatory)**
- Presentation in December: 15 minutes/3 marks out of 20
- Exam: written, 2 exercises (2x6 marks) + 1 quiz (5 marks)
  - **open book: you can bring any paper information and a calculator**

8

H05E1A/H05D9A Cryptography and Network Security Presentation on recent topic

- When:
  - 20-21 December
- How:
  - Group of 2 students
  - 15 minutes + 5 minutes questions
  - Need to be present for half a day (or 2 sessions) and ask questions
- What
  - Based on an article from a list (Toledo) or self-chosen topic
  - Initiative and broader interest (read more, test something)
- Evaluation
  - 3 marks out of 20
  - If you don't give a presentation, you **fail** the course
  - For September: contact the lecturer **well in advance** by email

9

Overview (1)

- Cryptography overview
- Symmetric cryptography (encryption)
- Mathematics of public key encryption
- Public key encryption
- Data authentication
- Entity authentication
- Key Establishment

10

Overview (2)

- Public Key Infrastructures
- Electronic Payment and blockchain
- Network security: TLS/IPsec/GSM/3G/4G

11

Exam schedule H05E1A and H05D9A

2 written exams (exam form imposed by KU Leuven)

Tue 16 Jan 09:00 – 12:00 (200L 00.07)
Tue 30 Jan 13:00 – 16:00 (ESAT/aula R)

12

Question 1a: modes of operation or public key (6/20)

The "plaintext-ciphertext chaining"-mode is defined as follows

C_i = E_K(P_i + C_{i-1} + P_{i-1})

with P_1, …, P_t the t plaintext blocks, C_1, … C_t the t ciphertext blocks, C_0=IV and P_0=0.

a) Indicate how you can decrypt.

b) Discuss the properties of this mode (hiding of patterns and repetitions, error propagation, synchronization, efficiency).

c) Indicate whether information leaks on the plaintext if too many plaintext blocks are encrypted under the same key (use as example the block cipher DES).

d) Does this mode offer data authentication in addition to data confidentiality?

13

Question 1b: modes of operation or public key (6/20)

Consider an RSA encryption system with modulus n=589.

a) Choose the smallest non-trivial public exponent. Compute the corresponding secret exponent.

b) Compute the ciphertext for the message `55'.

c) Decrypt the result with the Chinese remainder theorem and verify that you obtain the plaintext.

d) Are there any security issues if in RSA a common modulus is used between all the users (assume that the users do not know the factorization of this modulus), but every user obtains a different public and private exponent?

Expect a slightly more difficult question: RSA with 3 primes, variant of ElGamal, …

14

Question 2 (1) (6/20)

Consider the following protocol to establish a session key between a mobile device Alice (A) and a server Bob (B). Alice and Bob have an authentic copy of the public key of a common Certification Authority, but they do not share any other prior information.

$\text{Cert A} \,||\, r_A \rightarrow$

$\leftarrow E_{P_A}(k_B \,||\, \text{CertB}) \,||\, \text{Sig}_B\,(h(k_B)||\, \text{CertB}))$

$E'_{k_B}(k) \,||\, \text{Sig}_A(h(r_A)||\, \text{CertA})) \rightarrow$

The session key k is computed as $k = k_A \oplus k_B$.

A (B) the identity of the mobile device Alice (the server Bob)

CertA (CertB) the certificate of Alice (Bob)

P_A is the public encryption key of Alice

r_A is a 128-bit nonce generated by Alice

$E_{P_A}(.)$ asymmetric encryption computed with the public key of Alice

$\text{Sig}_X(.)$ digital signature computed with the private key of party X (digital signature with message recovery)

$E'_k(.)$ symmetric encryption with the secret key k

h() a cryptographic hash function.

15

Question 2 (2) (6/20)

$\text{Cert A} \,||\, r_A \rightarrow$

$\leftarrow E_{P_A}(k_B \,||\, \text{CertB}) \,||\, \text{Sig}_B\,(h(k_B)||\, \text{CertB}))$

$E'_{k_B}(k) \,||\, \text{Sig}_A\,(h(r_A)||\, \text{CertA})) \rightarrow$

a) Explain the role of the final step in the protocol and the actions Bob takes.

b) Which goals does the protocol achieve (entity authentication, implicit key authentication, key confirmation, explicit key authentication, anonymity w.r.t. third parties, key control, key freshness -- both for Alice and for Bob. Define each property in 1-2 sentences and justify your answer for each property with a few sentences.

c)] What is forward secrecy? Does this protocol offer forward secrecy?

d)] If necessary, modify the protocol to offer mutual entity authentication and mutual explicit key authentication. Try to avoid introducing new algorithms and minimize the number of rounds.

16

Question 3 (5/20)

Indicate which of the following five statements are correct. If they are wrong, explain why this is the case.

a) The encryption of information that contains redundancy will always result in data authentication as a side-effect.

b) The discrete logarithm problem modulo a 512-bit prime is approximately as hard as the factorization of 512-bit primes.

c) Finding a collision for an MDC with a 64-bit result can be performed using less than a day on a modern PC.

d) Bitcoin is an electronic cash system in which the users are fully anonymous w.r.t. each other but not w.r.t. the central bank that issues Bitcoins.

e) The RSA algorithm with a modulus and secret exponent of 128 bits is more secure than double-DES with a 112-bit key.

17

Two catch up lectures: please vote

1. Friday 29 10:35
2. Monday Oct 2 10:35
3. Tuesday Oct 3 10:35 x
4. Tuesday Oct 3 16:35 ?
5. Wednesday Oct 4 10:35
6. Wednesday Oct 4 14:00
7. Wednesday Oct 4 16:05 ?
8. Friday Oct 6 14:00?
9. Friday Oct 13 10:35
10. Monday Oct 16: 14:00?
11. Monday Oct 16 16:05 xx
12. Wednesday Oct 18 10:35

18