

**ECE 646
Cryptography
and
Computer Network Security**

Course web page:

**ECE web page → Courses →
Course web pages → ECE 646**

1

Jens-Peter Kaps

- Research and teaching interests:
 - Cryptography
 - Ultra-low-power cryptographic hardware design
 - Computer arithmetic
 - Efficient cryptographic algorithms
 - Computer and network security
- Contact:
 - S&T II – 213; e-mail: jkaps@gmu.edu
 - phone: 703-993-1611
- Office Hours:
 - Monday 2:00-3:00 pm, Thursday 7:30-8:30 pm

2

ECE 646

Part of:

MS in CpE

Network and System Security (required)
Computer Networks (elective)

MS in EE

Communications & Networks (elective)
Computers

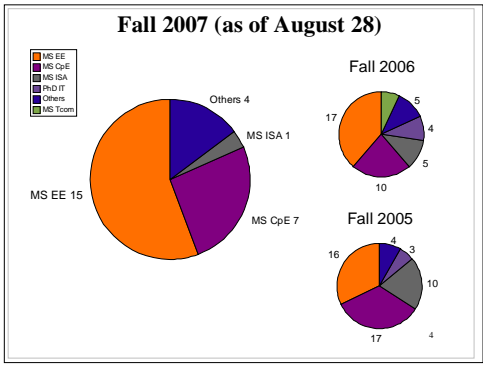
MS in Information Security & Assurance

MS in E-Commerce

Certificate in Information Systems Security

Ph.D. in Information Technology

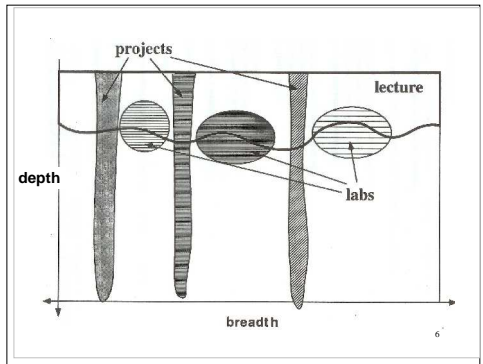
3



ECE646 Overview

- Lecture
- Homework (15%)
- Laboratory Exercises (15%)
- Project (15%)
- Midterm Examination (25%)
- Final Examination (30%)

5



Lecture

- viewgraphs / whiteboard
 - viewgraphs available on the web (please, extend with your notes)
- books
 - required (Stallings: *Cryptography and Network Security*)
 - online (Menezes, Oorschot, Vanstone, *Handbook of Applied Cryptography*)
- articles (CryptoBytes, RSA Data Security Conf., CHES, CRYPTO, etc.)
- web sites - **Crypto Resources**
standards, FAQs, surveys

7

Literature

- Serious
 - Trappe, Washington, *Introduction to Cryptography with Coding Theory*
 - Schneier, *Applied Cryptography*
 - Stinson, *Cryptography, Theory and Practice*
- Leisure
 - Kahn, *The Codebreakers*
 - Stephenson, *Cryptonomicon*
 - Harris, *Enigma*

8

Homework

- reading assignments
- theoretical problems (may require basics of number theory or probability theory)
- problems from the main textbook
- short programs (in C)
- literature surveys
- Analytical problems

9

Midterm exam

- ✓ 2 hours 30 minutes
- ✓ multiple choice test + short problems
- ✓ open-books, open-notes
- ✓ practice exams available on the web

Wednesday, October 24th

7:20 - 10:00

10

Final Exam

- 2 hours 45 minutes
- Multiple choice test + short problems
- open books, open notes

Wednesday, December 12th

7:30 – 10:15 pm

11

Laboratory

- 4-5 labs
- based on the GMU educational software, public domain cryptographic programs & libraries, or evaluation versions of commercial products
- done at home or in the ECE labs: software downloaded from the web
- based on detailed instructions
- grading based on written reports (answers to questions included in the instructions)

12

Tentative list of laboratory topics

1. Secure e-mail: PGP – Pretty Good Privacy
2. Historical ciphers - CrypTool
3. Properties of classical cryptosystems - Kryptos
4. Properties of public key cryptosystems - Kryptos
5. Secure e-mail: S/MIME

13

Project (1)

- original
- useful

- depth, originality
- based on additional literature
- based on something you know and are interested in
- only analytical
- teams of 2 students
- several project topics proposed by the instructor
- you can propose your own topic

14

Project (2)

- about four weeks to choose a topic and write the corresponding specification
- two progress report meetings with the instructor
- draft final presentation due same week as final report
- written report/article, 5-page IEEE style
due Wednesday December 5
- short conference-style oral presentations
Wednesday, December 19, 5:00-10:00 PM
- contest for the best presentation
- publication of reports and viewgraphs on the web

15

Project (3)

- Literature Search
 - Inspec, IEEE, ACM, Proceedings of Crypto, CHES, etc.
 - Up to 10 articles, full reference and abstract.
 - Electronic copy of ONE main reference to <mailto:gmuccc646@gmail.com>
 - Beware: Web pages, Google results, Class projects, etc. are in most cases not good references.

16

Project (4)

- Project reports/articles requirements
 - IEEE style
 - 5 pages maximum
 - appendices possible but do not influence the evaluation
 - 10 pt font, 2 columns
- Review of project reports
 - reviews done by your fellow students
 - reviews due Friday, December 14, 8:00 PM
 - final version of the report due Wednesday, December 19, 5:00 PM

17

Project (5)

Warning

- Don't copy someone else's work!
 - Citations are OK but must be referenced.
 - Graphs are better redrawn, explain them with your words.
 - Don't cite excessively.
- Copying someone else's work is a honor code violation and will be reported!

18

Project (4)

- Project presentations (Wednesday, December 19, 5:00-10:00 PM)
 - conference style, Johnson Center (tentatively)
 - several sessions, refreshments
 - attendance in at least three sessions required
 - open to general public (in particular, students from previous years), ECE seminar credit
 - 10 minutes for the presentation + 5 minutes for Q&A
 - time strictly enforced
- Detailed time line will appear on the class web page.

19

Follow-up courses

**Cryptography and Computer Network Security
ECE 646**

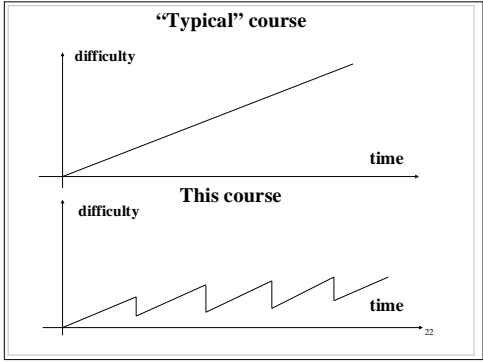
**Secure
Telecommunication
Systems
ECE 746**

**Computer Arithmetic
ECE 645**

20

Cryptography and Computer Network Security	Secure Telecommunication Systems
Modular integer arithmetic	Operations in the Galois Fields $GF(2^n)$
<ul style="list-style-type: none"> • Historical ciphers • Classical encryption (DES, IDEA, RC5, AES) • Public key encryption (RSA, DH, DSA) • Hash functions and MACs • Digital signatures • Public key certificates • Secure Internet Protocols <ul style="list-style-type: none"> - e-mail: PGP and S-MIME - www: SSL • Cryptographic standards 	<ul style="list-style-type: none"> • AES • Stream ciphers • Elliptic curve cryptosystems • Random number generators • Smart cards • Attacks against implementations (timing, power analysis) • Efficient and secure implementations of cryptography • Security in various kinds of networks (IPSec, wireless) • Zero-knowledge identification schemes

21



- ### Project Topics
- IDEA Cipher
 - AES Cipher
 - Number Field Sieve
 - Random Number Generators
 - Smart Cards
 - Kerberos
 - Side Channel Attacks
 - Cryptographic capabilities of Network Processors (e.g. Intel IXP)
- 23

- ### Projects - Detail
- Random Number Generation
 - Using Hardware / Software
 - True Random Numbers
 - Pseudo Random Numbers
 - Equal Probability / Unpredictability
 - Methods for generation
 - Randomness tests
 - Sources of randomness
 - Mathematical methods to improve randomness
- 24

Projects - Detail

- Security Protocols for Wireless Networks
 - Sensor Networks
 - Ad-Hoc Networks
 - Static Topography
 - With Mobility
 - Smart Dust
 - Prey by Michael Crichton

25

Projects - Detail

Security of RFIDs

Challenge:

Cryptographic operations need to be implemented using up to 4000 gates, consuming less than 20 μ W

- new algorithms
- new protocols

Protection of privacy

26