

**ECE 297:11**  
**Reconfigurable Architectures**  
**for Computer Security**

**Course web page:**  
<http://mason.gmu.edu/~kgaj/ECE297>

---

---

---

---

---

---

---

---

**Instructors:**

**Kris Gaj (GMU)**

**Tarek El-Ghazawi (GWU)**

**TA:**

**Pawel Chodowiec (GMU)**

---

---

---

---

---

---

---

---

**Kris Gaj**

George Mason University  
Science & Technology II, room 223  
kgaj@gmu.edu, (703) 993-1575

**Tarek El-Ghazawi**

George Washington University  
Phillips Hall, room 624D  
tarek@seas.gwu.edu, (202) 994-2607

**Pawel Chodowiec**

George Mason University  
Science & Technology II, room 220  
pchodow1@gmu.edu, (703) 963-3788

---

---

---

---

---

---

---

---

**Most-related GMU courses**

**ECE 646**  
**Cryptography and Computer  
Network Security**

**ECE 545**  
**Introduction to VHDL**

**ECE 746**  
**Secure Telecommunication  
Systems**

**ECE 645**  
**Computer Arithmetic**

---

---

---

---

---

---

---

---

**Cryptography and Computer  
Network Security**

- Historical ciphers
- **Classical encryption (DES, IDEA, RC5, AES)**
- **Public key encryption (RSA)**
- Message authentication and Hash functions
- Digital signatures
- Public key certificates
- Secure Internet Protocols
  - e-mail: PGP and S-MIME
  - www: SSL
- Cryptographic standards
- Key escrow encryption
- Quantum cryptography

**Secure  
Telecommunication Systems**

- Stream ciphers
- **Elliptic curve cryptosystems**
- Smart cards and PCMCIA cards
- Attacks against implementations (timing, power analysis)
- **Efficient and secure implementations of cryptography**
- Security in various kinds of networks (IPSec, ATM, wireless)
- Passwords, authentication tokens
- Zero-knowledge identification schemes
- Biometric methods

---

---

---

---

---

---

---

---

**Specific to this course**

- supports research rather than competes with the research
- intense
- project oriented
- flexible
- extendible into future thesis and sponsored-research work

---

---

---

---

---

---

---

---

### Topics (1)

#### Part I Introduction & secret-key cryptosystems

Instructor: Kris Gaj

1. Security services. Basic concepts of cryptology.
2. Types of cryptosystems. Implementation of security services.
3. Mathematical background. Modular arithmetic.
4. Older secret key ciphers: DES, Triple DES, IDEA, RC5, Skipjack.
5. New encryption standard AES, AES candidates.
6. Implementing basic operations of secret key ciphers in software & hardware.
7. Modes of operation of secret-key ciphers.  
Hardware architectures for secret key ciphers.

---

---

---

---

---

---

---

---

### Topics (2)

#### Part II Computer arithmetic in reconfigurable hardware

Instructors: Tarek El-Ghazawi, Pawel Chodowiec, Kris Gaj

1. Architectures of the current generation of reconfigurable devices.
2. Fast addition. Ripple-carry and carry-lookahead adders.
3. Multioperand addition.
4. Fast multiplication. Tree and array multipliers.
5. Systolic arrays.
6. Pipelining.
7. Design flow and tools used for design of cryptographic modules.

---

---

---

---

---

---

---

---

### Topics (3)

#### Part III Public key cryptosystems

Instructor: Kris Gaj

1. Public-key cryptosystems: RSA.
2. Implementation of RSA. Fast modular exponentiation. CRT.
3. Public key cryptosystems based on the discrete logarithm.
4. Elliptic curve cryptosystems over  $GF(p)$ .
5. Operations on large integers. Montgomery Multiplication.
6. Galois Fields  $GF(2^m)$ . Implementing operations in the Galois Fields in hardware.
7. Elliptic Curve Cryptosystems over  $GF(2^m)$  with polynomial representation.
8. Elliptic Curve Cryptosystems over  $GF(2^m)$  with normal basis representation.

---

---

---

---

---

---

---

---

**Proposed schedule (1)**

- Lecture Part I - June 3 - June 13
- Project I - June 15 - July 19
- Lecture Part II - TBD
- Exam - July 15
- Final Project I presentations & reports - July 19
- **Grading - July 22**
- Lecture Part III - July 22-August 1
- Project II - August 1 - August 23
- Final Project II presentations & reports - TBD

---

---

---

---

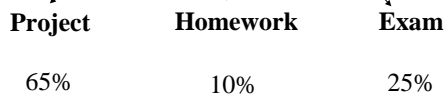
---

---

---

---

**Grading**



---

---

---

---

---

---

---

---

**Project**

- groups of 1-3 students
- topics suggested by the instructors
- implementation of a cryptosystem in reconfigurable hardware using VHDL or Verilog HDL
- HDL code
  - fully verified using available test vectors and public domain software implementations of cryptographic algorithms.
  - experimentally tested using FPGA board, such as SLAAC-1V or Firebird, or reconfigurable hypercomputer.

---

---

---

---

---

---

---

---

### **Resources**

- Standards & specifications
  - NIST Cryptographic Toolkit
  - AES
  - IEEE P1363
- Software cryptographic libraries
  - Crypto++
  - MIRACL
- FPGA resources
- Cryptographic dictionary

---

---

---

---

---

---

---

---

### **Cryptographic dictionary project**

- English
  - Polish
  - French
- 
- Arabic
  - Vietnamese
  - Hindi
  - Nepali
  - ?

---

---

---

---

---

---

---

---

### **Handling the code**

- export restrictions
- no hardware cryptographic modules in public domain
- protection access to your code
- transfer of codes on diskettes and using PGP
- rules regarding sharing the codes

---

---

---

---

---

---

---

---