Advanced Topics in Information Security

Applied Cryptosystems:
Techniques & Architectures

Adnan Gutub
aagutub “at” uqu.edu.sa

Catalogue Description

- Introduction to encryption and information hiding.
- Mathematical Foundation of Cryptography.
- Private and Public key Cryptosystems.
- Key Protocol and Management.
- Ciphers.
- Advanced Encryption Standard.
- Digital Signatures.
- Elliptic Curve Cryptosystems.
- Architectures of Cryptosystems and Processors.

Grading Policy:

- Attendance 5%
- Assignments 15%
- Midterm Exam 20%
- Final Exam 40%
- Project 20%
  - Paper Summary & Discussion 5%
  - Testing & Verification 5%
  - Modification & Comparison 5%
  - Report & Presentation 5%

Weekly Progress

Week	Deadline	Task
3	Saturday 15 February 2014	HomeWork 1 = HW1
4	Saturday 22 February 2014	HomeWork 2 = HW2
5	Saturday 1 March 2014	3 papers for instructor to choose your focus paper
6	Saturday 8 March 2014	Paper Selection; HomeWork 3 = HW3
7	Saturday 15 March 2014	**Midterm Exam** Understand Focus paper : submit one page summary report
8	Saturday 22 March 2014	testing & verification: brief report
	Saturday 29 March 2014	Midterm Break
9	Saturday 5 April 2014	HomeWork 4 = HW4
10	Saturday 12 April 2014	Modification & Comparison : brief report
11	Saturday 19 April 2014	HomeWork 5 = HW5
12	Saturday 26 April 2014	
13	Saturday 3 May 2014	Report & Presentation : **Final Report**
14	Saturday 10 May 2014	OUT
15	Saturday 17 May 2014	
16	18-29 May 2014	Final Week
17		

Paper Summary & Discussion 5%

- Each student needs to give the instructor three (3) papers to choose from for their focus study. These three papers should be submitted by end of ***Week 5***
- The instructor will assign a paper for the student to work on by ***Week 6.***
- The chosen paper should be understood in depth and a one page summary report is to be submitted. The report should be in the students *own words and not copied from the resources.* This summary report should be submitted by the end of ***Week 7***
- Note that the papers should be on related topic to the course, from reputable journals or conferences, and ***should not be more than three years old.***

Testing & Verification 5%

- To proof understanding the chosen paper, it should be tested & verified by the student.
- These testing & verification are to be completed by ***week 8***

Modification & Comparison 5%

- A modification to the idea is to be agreed upon.
- This modification is to be tested and verified.
- The modification needs to be compared to the original idea tested results.
- This should be ready by ***week 10.***

Report & Presentation 5%

- ¨ Title:
- ¨ Your Name
- ¨ Abstract: (to briefly describe your work and improvement)
- ¨ Keywords:
- ¨ Introduction: (importance and possible applications, previous work, your exact achievements, and briefing of the sections flow within the document)
- ¨ Brief Theoretical Background and/or Available Methods: (presented different techniques as examples)
- ¨ Detailed description of the studied work: (describe the idea, procedure, algorithm and your implementation tests)
- ¨ Your improvement: (describe all updates and implementation of your improvement)
- ¨ Detailed comparisons:
- ¨ Conclusion
- ¨ Acknowledgment: Thank UQU; Example: "Thanks to Umm Al-Qura University for supporting this work."
- ¨ References

Considerations: What do we want?

- Privacy of our data
- Integrity of our data
- Usability of our system/data

Concepts

- Confidentiality of data
- Integrity of data
- Authentication of users

What Functionality Is Needed?

- Authentication -- who user is
- Authorization -- who is allowed to do what
- Enforcement -- make sure people do what they are supposed to do

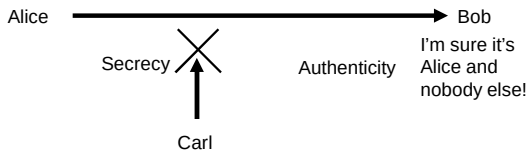
Definitions

- Secrecy (Confidentiality)
  - Diary Lock
- Authenticity
  - Hi it's Bob.
  - Prove it Dude...

Definition Examples

- Secrecy
  - Alice sends message to Bob. Carl intercepts the message... but can't read
- Authenticity
  - Alice sends message to Bob. Bob can verify that Alice is the sender.

The Big Picture



Methods

- Cryptography
  - Converting messages to unreadable forms... Unconverting it back to the readable form
- Steganography
  - Hiding the existence of a message

Steganography

Null Cipher

Fishing freshwater bends and saltwater coasts rewards anyone feeling stressed. Resourceful anglers usually find masterful leapers fun and admit swordfish rank overwhelming anyday.

Send lawyers, guns, and money.

Invisible Ink

- Write with lemon juice and a toothpick/ cotton swab. Let the paper dry.
- Heat the paper with an iron to reveal the hidden message.

Cryptography

Greek: kryptos + graphein → hidden writing