

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 & Quizzes 20%
- Project 50%
 - Paper Summary & Discussion 10%
 - Testing & Verification 10%
 - Modification & Comparison 10%
 - Report & Presentation 20%
- Exam 25%

Paper Summary & Discussion 10%

- 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 10%

- 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 10%

- 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 20%

- - 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

Fishing freshwater be~~r~~ds and ~~s~~altwater co~~a~~sts
re~~w~~ards any~~o~~ne feel~~i~~ng st~~r~~essed. Re~~s~~ourceful
an~~g~~lers us~~u~~ally fi~~n~~d ma~~s~~terful le~~a~~pers fun and ad~~m~~it
sw~~o~~rdfish ran~~k~~ over~~w~~helming any~~d~~ay.

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