

## Syllabus

*Fall 2009*

### Objectives:

The course is intended to provide an introduction to modern cryptography. You will learn how various cryptographic schemes work from a theoretical and an applied standpoint. You will learn about the different classes of algorithms. You will review the concept of public keys and apply this concept with GnuPG and OpenSSL. You will learn about certificates and understand TLS. You will review and expand your knowledge of arithmetic; you will see how choosing random prime numbers can be critical. You will see several algorithms, including AES and RSA.

### Class Language:

The class will take place in English; this includes the exams and in-class participation.

### Instructors:

#### *John Cagnol*

E-mail: john@cagnol.com.

GnuPG Key ID 4AE54F4C.

Fingerprint: 7067 5B4E 8525 5A70 2EF3 895E 27E4 232B 4AE5 4F4C

Phone: 01 41 16 71 88. Fax: 01 41 16 71 71.

Throughout the first part of the fall semester, office hours will be held on Tuesday nights from 5:30 to 6:30 with an exception on October 13th: office hours will be held the day before, on Monday October 12th from 5:30 to 6:30.

#### *Amaury Darsh*

E-mail: amaury.darch@devinci.fr.

GnuPG Key ID EF82D31D.

Fingerprint: 47B2 D23C 6AFB 1891 4860 2F77 9986 1305 EF82 D31D

Phone: 01 41 16 74 24. Fax: 01 41 16 71 71.

### Mini-Project:

You will be given a mini-project on September 21st that will have to be completed and turned in by October 5th at 1pm CET at [www.cagnol.com/hws](http://www.cagnol.com/hws). Meeting deadlines is important in the professional world. A penalty for late homework will be applied as follows: 2 points per hour.

### Exam:

The final exam will take place during the second week of November. It will last 2 hours. Documents will be allowed (with no limitation on type or number). You will not be allowed to use a calculator or any other electronic device. If computations are required, the necessary computing equipment will be provided by the proctors at the beginning of the exam.

### **In-class Participation:**

In-class participation is important to create the best possible learning environment and to improve your classroom experience. Throughout the class, instructors will ask questions or give puzzles. Answers to these questions will be graded in an in-class participation grade. See the section “challenge” for an additional twist on this grade.

### **Grading:**

The overall grade will be computed as follows:

15 % Mini-project  
15 % In-class participation  
70 % Final exam

The highest possible score is 20. Passing grade is 10. The overall grade will be rounded to the nearest half-point. If the overall grade is 9.5, it will be replaced by 10 and you will pass.

### **Reference:**

There is no required textbook. However, further information can be obtained in:

*Handbook of Applied Cryptography* by Alfred Menezes, Paul van Oorschot and Scott Vanstone. CRC-Press, 1996. ISBN 978-0-8493-8523-0

The call number of this book at the university library is INFO 23 MENE. It can be found on the second floor.

Chapters of this book can be downloaded for free at <http://www.cacr.math.uwaterloo.ca/hac/> and used in compliance with the licence agreement.

### **Class Website:**

<http://www.cagnol.com/promotion2010/3906>

The class website is also accessible through Blackboard DeVinci.

### **Challenge:**

We consider the following communication:

GGVRM ELCWV XAWYN O1OJJ YOPLQ IOJ CJ OWVOO LWONM CHBZB VSXSD GOKZI XWAE  
TDMLN IOJCD RYOEC IOSPT OLWOT SMOAM SXMDN SJOEJ OJMNJ VVOJJ YOAFX GWAD

If you find the secret message, everybody in the class will receive a *minimum* of 14 out of 20 for the in-class participation grade. In addition, the first person to send the secret message to [amaury.darsh@devinci.fr](mailto:amaury.darsh@devinci.fr) will get a brand new INTEL Atom board (add memory and a hard drive and you’ve got a computer). Thus this challenge can both be a class effort or an individual one.

Whether you decide to collaborate with your fellow classmates or not is left up to you: in one case you increase your chances to break the code and subsequently guarantee having *at least* 14 out of 20 in the in-class participation grade, in the other case you increase your chances to be the first one to break the code and to get the Atom board. Whatever you decide... Good luck!