Pôle Universitaire Léonard de Vinci
ESI GI 3906 – Cryptography

Semester 9 – Year 2008-2009
ESILV – Class of 2009

Syllabus

Fall 2008

Objectives:

The course is intended to provide an introduction to modern cryptography. You will learn how various cryptographic schemes work from a theoritical 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 DES, AES, RSA, DH, SHA-1 and MD5.

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 to 6:30. There will be no office hours during the vacation week and national holidays.

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.

Exams:

The midterm will take place on October 7th. It will last 30 minutes. No documents will be allowed for the midterm.

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).

For both exams, 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 % Mid-term exam
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://aldebaran.devinci.fr/∼cagnol/gi3906

Challenge:

We consider the following communication:

```
PBATE NGHYN GVBAF BAOER NXVAT GURSV EFGYB PXGUR ERVFN FRPBA QBARG BOERN XCHOY
VPXRL VF3SS SSSSS SSSSS SSSSS S1P00 00000 00000 00000 P8QFR CNENG BEPSQ 41091
RAQBS XRLZR FFNTR UNF3O YBPXF 39771 55143 288P8 SNN59 2P5RN 4SNSS 741P3 46521
RFRCN ENGBE 1OPNQ 49Q7P QPR70 33575 777N3 404RO 0SR10 S675N FRCNE NGBE4 8PRQR
SPPQN 76S77 84OOR 469NS 463OQ S7Q14 2OS4R AQBSZ RFFNT RTBBQ YHPX
```

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 john@cagnol.net will get a USB-remote control with laser pointer. 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 USB-remote control with laser pointer. Whatever you decide... Good luck!