Date: Monday, January 14, 2002
Prof.: Dr. Jean-Yves Chouinard
Location: Colonel-By Hall, room A-610

ELG-5373 (92.515) Secure Communications and Data Encryption

Suggested Term Paper Subjects

1. Information theory and communication secrecy [Sti95].
2. Complexity and NP-complete problems [LV93].
3. Differential cryptanalysis [BS93].
4. Comparative study of candidate AES algorithms (Web).
5. Efficient sorting and searching algorithms [Knu73].
6. Elliptic curve cryptography [Gar01].
7. Factoring algorithms [BW00].
8. Number theory and primality testing [BW00].
9. Identity verification methods and schemes [DP84].
10. Key management and distribution schemes [Sta99].
11. Secure communications for wireless applications [Tor92].
12. Proof of knowledge with minimum information disclosure [Bra88].
13. Digital watermarking [Ke00].
14. Quantum cryptography [Bra88, WC98].

References

[Bra88] G. Brassard. *Modern Cryptology: A Tutorial*. Lecture Notes in Computer Science. Springer-Verlag, New-York, 1988.

[BS93] E. Biham and A. Shamir. *Differential Cryptanalysis of the Data Encryption Standard*. Springer-Verlag, New-York, 1993.

[BW00] D. Bressoud and S. Wagon. *Computational Number Theory*. Key College Publishing, Emeryville, California, 2000.

[DP84] D.W. Davies and W.L. Price. *Security for Computer Networks*. John Wiley and Sons, New-York, 1984.

[Gar01] P. Garrett. *Making, Breaking Codes: An Introduction to Cryptology*. Prentice-Hall, Upper Saddle River, New-Jersey, 2001.

[Ke00] S. Katzenbeisser and F.A.P. Petitcolas (editors). *Information Hiding Techniques for Steganography and Digital Watermarking*. Artech House, Norwood, Massachusetts, 2000.

[Knu73] D.E. Knuth. *The Art of Computer Programming: Sorting and Searching (volume 3)*. Addison-Wesley, Reading, Massachusetts, 1973.

[LV93] M. Li and P. Vitányi. *An Introduction to Kolmogorov Complexity and its Applications*. Texts and Monographs in Computer Science. Springer-Verlag, New-York, 1993.

[Sta99] W. Stallings. *Cryptography and Network Security: Principles and Practice*. Prentice-Hall, Upper Saddle River, New-Jersey, second edition, 1999.

[Sti95] D.R. Stinson. *Cryptography: Theory and Practice*. CRC Press, Boca Raton, USA, 1995.

[Tor92] D.J. Torrieri. *Principles of Secure Communication Systems*. Artech House, Norwood, Massachusetts, second edition, 1992.

[WC98] C.P. Williams and S.H. Clearwater. *Explorations in Quantum Computing*. Telos. Springer-Verlag, New-York, 1998.