Cryptographic Protocols

(Alice and Bob in Wonderland)

60 hours

Dean Rosenzweig

Mathematical Preliminaries

Number theory and algebra: Z_p, Z_p^*, chinese remaindering, φ and Euler's theorem, polynomials, finite fields.

Decidability and complexity: machine models, complexity classes, P, NP, PSPACE, EXPTIME, reductions, hard and complete problems.

Algorithmic problems of algebra and number theory: factorization, primality, RSA–problem, quadratic residuality, roots in Z_m, discrete logarithms, Diffie–Hellman problem, sum of subsets, factoring polynomials over finite fields.

Pseudorandom sequences: statistical methods, complexity based approach, cryptographic methods.

Logic: propositions and predicates, Hintikka and Henkin sets, interactive and 0–knowledge proofs, a brief course in modal logic (modalities, Kripke structures and frames, correspondence), logics of knowledge and belief: individual, shared, common and distributed knowledge and belief.

Cryptographic Primitives

Basic notions of cryptography

One-way functions: CRC, MD5, SHA.

Symmetric algorithms: DES, IDEA, AES.

Asymmetric algorithms: RSA, Diffie–Hellman, elliptic curves.

Signatures and certificates: RSA, DSA, x509

Attacking algorithms: statistic analysis, searching, dictionary attacks, fast factoring, differential cryptoanalysis.

Cryptographic Protocols

Basics of protocols: Alice, Bob and other characters, Dolev-Yao notation and assumptions.

Authentication and secret exchange: a catalogue of protocols.

Attacking protocols (education of girls on the Internet): reflection, recycling, parallel sessions, exploits of cryptographic weaknesses, attacking machines.

Formal models of protocols: multiset rewriting, process calculi, strand spaces, abstract state machines.

Decidability and complexity of protocol properties: undecidability of security, lower complexity bounds for restricted protocols.

Reasoning about protocols: inductive reasoning on operational models, logics of knowledge and belief for proving properties of protocols.

Essential References

R. Fagin, J.Y. Halpern, Y. Moses, M.Y. Vardi, *Reasoning About Knowledge*, MIT Press 1995, `http://www.cs.rice.edu/vardi/papers/index.html/`

A. Menezes, P. van Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, CRC Press 1996, `http://www.cacr.math.waterloo.ca/hac`.

Recommended References

`http://theory.lcs.mit.edu/rivest/crypto-security.html`

P. Blackburn, M. de Riejke, Y. Venema, *Modal Logic*, 1999, `http://www.illc.uva.nl/mdr/Publications/modal-logic.html`

J. Clark, J. Jacob, *A Survey of Authentication Protocol Literature*, 1997, `http://www-users.cs.york.ac.uk/jac/papers/drareviewps.ps`

O. Goldreich, *Foundations of Cryptography (Fragments of a Book)*, `http://theory.lcs.mit.edu/oded/frag.html`

B. Schneier, *Applied Cryptography*, Wiley 1996, `http://www.counterpane.com/applied.html`.

D. Stinson, *Cryptography: Theory and Practice*, CRC Press 1997, `http://www.cacr.math.uwaterloo.ca/dstinson/CTAP.html`

Software for Experimenting

`http://www.cs.auckland.ac.nz/pgut001/cryptlib/` (C/C++)

`http://www.openjce.org/` (Java)