

**Project References
collected by students
as of
09/22/04**

Software Projects - Fall 2004

Educational software

KRYPTOS - Educational software for a cryptographic laboratory.

Noah Dowd - noahdowd@yahoo.com

1. [Open Source] www.gnu.org/copyleft/gpl.html GNU General Public License
2. [Open Source] www.phpbb.com Software for open source bulletin board maintenance. Links to databases, etc.
3. [Open Source] www.developer.com "Bug Tracking Made Simple", Yaron Sinai
4. [Open Source] www.onlamp.com "Open Source Security: Still a Myth", John Viega
5. Network Security with OpenSSL: Cryptography for Secure Communications, John Viega, Matt Messier, Pravir Chandra, 2002
6. SSL and TLS: Designing and Building Secure Systems, Eric Rescorla, 2001
7. OpenSSL website www.openssl.org
8. OpenSSL examples www.rtfm.com/openssl-examples/
9. KRYPTOS Manual
<http://mason.gmu.edu/~aabushar/code/KRYPTOS.pdf>
10. SSLeay Documentation (predecessor to OpenSSL)
www.columbia.edu/~ariel/ssleay/

Chandrika Lanka - clanka@gmu.edu

1. William Stallings, "Cryptography and Network Security, Principles and Practice", Third Edition Chapter 8, Chapter 9
2. Springer Verlag, "Number Theory for Computing", Second Edition.

3. Laboratory Instructions for ECE 636, KRYPTOS MANUAL, URL:
http://ece.gmu.edu/courses/ECE636/labs_S04/lab1_instruction.pdf
4. Literature on Algorithms
 - DES: <http://www.itl.nist.gov/fipspubs/fip46-2.htm>
 - RSA:
http://www.rsasecurity.com/rsalabs/rsa_algorithm/index.html
 - MD5: <http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc1321.html>
 - AES: <http://csrc.nist.gov/CryptoToolKit/aes>
 - RSA: <http://www.rsasecurity.com/rsalabs/cryptobytes>
5. Randomness tests literature survey
<http://www.ciphersbyritter.com/RES/RANDTEST.HTM>
6. Crypto API, Library for Cryptographic Applications.,
http://cnscenter.future.co.kr/crypto/open_src.html#API
Includes Crypto++ Library, www.eskimo.com/~weidai/cryptlib.html
7. Bruce Schneier's Crypto Bibliography,
<http://www.schneier.com/biblio/year-1992.html>
8. Ron Rivest's Web page for links to resources for software, articles and publications, <http://theory.lcs.mit.edu/~rivest/crypto-security.html>
9. Ueli Maurer: A Universal Statistical Test for Random Bit Generators
Advances in Cryptology - CRYPTO '90, Lecture Notes in Computer Science, Springer-Verlag, vol. 537, pp. 409-420,
10. A Statistical Test Suite for random and pseudorandom number generators for cryptographic applications. NIST Special Publication 800-22. URL: <http://csrc.nist.gov/publications/nistpubs/800-22/sp-800-22-051501.pdf>
11. Ueli Maurer, "Some Number-theoretic Conjectures and their relation to generation of cryptographic primes", Cryptography and Coding II, Oxford University Press, 1992.
<http://citeseer.ist.psu.edu/cache/papers/cs/785/ftp:zSzzSzftp.inf.e thz.chzSzpubzSzpublicationszSzpaperszSztizSzisczSzcir.pdf/maurer92some.pdf>
12. Literature on Algorithms
 - DES: <http://www.itl.nist.gov/fipspubs/fip46-2.htm>
 - RSA:
http://www.rsasecurity.com/rsalabs/rsa_algorithm/index.html
 - MD5: <http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc1321.html>

- AES: <http://csrc.nist.gov/CryptoToolkit/aes>

RSA: <http://www.rsasecurity.com/rsalabs/cryptobytes>

Jeremy Nightingale - jsn1776@yahoo.com

1. Narasimhan, B. DIEHARD [Online]. Available from World Wide Web: (<http://stat.fsu.edu/~geo/diehard.html>).
2. Walker, John. October 20, 1998. ENT: A Pseudorandom Number Sequence Test Program [Online]. Available from World Wide Web: (<http://www.fourmilab.ch/random/>).
3. Hellekalek, Peter. pLab Tests for Random Numbers. Available from World Wide Web: (<http://crypto.mat.sbg.ac.at/tests/>).
4. Eastlake, Donald E., Stephen D. Crocker, and Jeffrey I. Schiller. December 1994. RFC 1750 - Randomness Recommendations for Security [Online]. Available from World Wide Web: (<http://www.faqs.org/rfcs/rfc1750.html>).
5. Gupta, Rajiv, Scott Smolka, and Shaji Bhaskar. On Randomization in Sequential and Distributed Algorithms. *ACM Computing Surveys*, Vol. 26, No. 1, March 1994.
6. Rukhin, A., J. Soto, J. Nechvatal, and M. Smid. "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications." NIST Special Publication 80022.
7. Soto, Juan. *Statistical Testing of Random Number Generators*. National Institute of Standards & Technology.
8. Smith III, Julius O. January 1, 2004. *Mathematics of the Discrete Fourier Transform (DFT)* [Online]. California: Stanford University, Center for Computer Research in Music and Acoustics (CCRMA), Department of Music. Available from World Wide Web: (<http://ccrma.stanford.edu/~jos/r320/>).
9. Manno, Istvan. 1999. *Introduction to the MonteCarlo Method*. Hungary: Adademiai Kiado.
10. Bendat, Julius S. and Allan G. Piersol. 2000. *Random Data: Analysis and Measurement Procedures*, 3rd ed. New York: John Wiley & Sons, Inc.

Robert Salembier - rsalembi@gmu.edu

1. Open Source site: <http://www.opensource.org/>
2. White paper on converting to Open Source:
<http://www.hecker.org/writings/setting-up-shop.html>
3. Paper on why to going to open source;
http://www.dwheeler.com/oss_fs_why.html
4. Open Source GPL compliant software:
<http://www.dwheeler.com/essays/gpl-compatible.html>
5. CVS Concurrent Version System Book(how to manage updates):
<http://cvsbook.red-bean.com/>
6. Open Source Software Institute: <http://www.oss-institute.org/>
7. Kryptos: <http://mason.gmu.edu/~aabushar/download.htm>
8. Kryptos Manual: <http://mason.gmu.edu/~aabushar/code/KRYPTOS.pdf>
9. Crypto++ Library: <http://www.eskimo.com/~weidai/cryptlib.html>
10. GNU software page: <http://www.fsf.org/>

Paul Southerington - psouther@gmu.edu

1. SourceForge: <http://sourceforge.net/>
2. OpenSSL web site: <http://www.openssl.org/>
3. Open Source Initiative: <http://www.opensource.org/>
4. KRYPTOS web site: <http://mason.gmu.edu/~aabushar/download.htm>
5. St. Laurent, Andrew, Understanding Open Source and Free Software Licensing, Reilly & Associates, 2004
6. Concurrent Versions System: <https://www.cvshome.org/>
7. Bugzilla bug tracking: <http://www.bugzilla.org/>
8. Crypto++ Library 5.2.1: <http://www.eskimo.com/~weidai/cryptlib.html>
9. WineLib Users Guide: <http://www.winehq.org/site/docs/winelib-user/index>
10. Schneier, Bruce, Applied Cryptography
11. Stevens, W. Richard, Advanced Programming in the UNIX Environment
12. Menezes, Alfred et. al., Handbook of Applied Cryptography

CAMERA - Educational software for experiential learning of cryptography.

Public-key cryptosystems

Generating large primes for cryptographic applications.

Noah Dowd - noahdowd@yahoo.com

1. www.mersenne.org/prime.htm Website for internet prime number search
2. Cryptography and Network Security: Principles and Practices, William Stallings, 2003, Sections 8.1, 8.2, 8.3, 8.4
3. www.programmersheaven.com/2/Art_CSharp_8 C++ code for the Sieve of Eratosthenes
4. www.crypto-world.com/FactorCode.html Code for factoring primes
5. www.mathworld.wolfram.com References for prime number characteristics and algorithms
6. Introduction to Algorithms, Thomas Cormen, Charles Leiserson, Ronald Rivest, Cliff Stein, 2003
7. "The Quadratic Sieve Factoring Algorithm", Eric Landquist, 2001, www.math.uiuc.edu/~landquis/quadsieve.pdf
8. "Automatic Generation of Prime Factorization Algorithms Using Genetic Programming", David Michael Chan, 2002. www.genetic-programming.org/sp2002/Chan.pdf
9. Pomerance, C. "Analysis and Comparison of Some Integer Factorization Algorithms." In Computational Methods in Number Theory, Part 1 (Ed. H. W. Lenstra and R. Tijdeman). Amsterdam, Netherlands: Mathematisch Centrum, pp. 89-139, 1982.
10. Pomerance, C. "A Tale of Two Sieves." Not. Amer. Math. Soc. 43, 1473-1485, 1996.

Chandrika Lanka - clanka@gmu.edu

1. Menezes, P. Van Oorschot, and S. Vanstone, "Handbook of Applied Cryptography", Chapter 4 on Public Key parameters. Chapter 2 on Mathematical Background
2. Lecture Notes on Cryptography www-cse.ucsd.edu/users/mihir/papers/gb.pdf
3. Institute of Theoretical Computer Science, "Generation of Prime Numbers" <http://www.crypto.ethz.ch/research/ntc/gpn/>.
4. Thesis from NJIT

- <http://archives.njit.edu/vol01/etd/2000s/2001/njit-mt2001-030/njit-mt2001-030.pdf>
5. Korea Information Security Agency : A Gateway to Public-Key Cryptography
<http://www.kisa.or.kr/technology/sub1/index-PKC.htm>
 6. Advances in Cryptology, Proceedings of EuroCrypt '84
<http://dsns.csie.nctu.edu.tw/research/crypto/HTML/E84.HTM>
 7. CITY's Cryptography and Network Security Resources Page
www.city.academic.gr/acm/crypto-page/default.htm
 8. RSA Reference Library and Website
<ftp://ftp.rsa.com>
 9. Publications, "Fast generation of Prime Numbers and Secure Public Key Cryptographic Parameters".
http://citeseer.ist.psu.edu/cache/papers/cs/784/ftp:zSzzSzftp.inf.e thz.chzSzpubzSzpublicationszSzpaperszSztizSzisczSzPrime_Generation.pdf/maurer94fast.pdf
 10. Publication, "A Probable prime test with high confidence".
<http://citeseer.ist.psu.edu/cache/papers/cs/3470/http:zSzzSzwww.c lark.netzSzpubzSzgranthamzSzpseudozSzpseudo2.pdf/a-probable-prime-test.pdf>
 11. Implementing Cryptography: Cryptographic Toolkits and Libraries
<http://www.cgisecurity.com/owasp/html/ch13s06.html>
 12. Bosselaers, B. Preneel (Eds.), "Integrity Primitives for Secure Information Systems: Final Report of RACE Integrity Primitives Evaluation, RIPE-RACE 1040," chapter 9, "RSA Key Generation," Springer 1995, pp. 213-231.
 13. Publication, "Strong primes are easy to find"
<http://dsns.csie.nctu.edu.tw/research/crypto/HTML/PDF/E84/216.PDF>
 14. Publication, Efficient Generation of Prime Numbers,
www.gemplus.com/smart/r_d/publications/pdf/JPV00gen.pdf

Rohan Misquith - rmisquit@gmu.edu

1. http://www.enstimac.fr/Perl/perl5.6.1/site_perl/5.6.1/Crypt/Primes.html
2. <http://www.awprofessional.com/articles/article.asp?p=170808&seqNum=3>

3. <ftp://ftp.inf.ethz.ch/pub/crypto/publications/Maurer95a.pdf>
4. <http://www.cacr.math.uwaterloo.ca/hac/about/chap4.pdf>
5. <http://theory.lcs.mit.edu/~rivest/RivestSilvermanAreStrongPrimesNeededForRSA.pdf>
6. <http://www.sans.org/rr/papers/20/969.pdf>
7. <http://www.cccure.org/Documents/Cryptography/S-crypt03.pdf>
8. http://www.gemplus.com/smart/r_d/publications/pdf/JPV00gen.pdf
9. http://www.eas.asu.edu/~cse450sp/projects/final_P12.doc
10. http://bornova.ege.edu.tr/~enis/bildiri/PrimeTestingAndSecurity_01042002.doc
11. <http://www2.arnes.si/~massvega/documents/ke-2003/Cryptography.doc>
12. C. Couvreur and J.-J. Quisquater. An introduction to fast generation of large prime numbers. Philips J. Research 37, pages 231-264, 1982

Jeremy Nightingale - jsn1776@yahoo.com

1. Shade, Eric, February 2002. Ready for Prime Time? Southwest Missouri State University, JCSC 17, 3.
2. Herkommer, Mark. 1999. Number Theory: A Programmer's Guide. New York: McGrawHill.
3. Caldwell, Chris. Primality Proving 1: A Quick Introduction [Online]. Available from World Wide Web: (<http://www.utm.edu/research/primes/prove/merged.html>).
4. Yan, Song Y. 2002. Number Theory for Computing, 2nd ed. Germany: SpringerVerlag.
5. Bernstein, Daniel J, February 12, 2004. Distinguishing Prime Numbers from Composite Numbers: The State of the Art in 2004. Department of Mathematics, Statistics, and Computer Science, The University of Illinois at Chicago.
6. Burton, David M. 1998. Elementary Number Theory, 4th ed. McGrawHill.
7. Agrawal, Manindra and Somenath Biswas, July 2003. Primality and Identity Testing via Chinese Remaindering. Journal of the ACM, Vol. 50, no. 4.
8. McGregorDorsey, Zachary S. Methods of Primality Testing. MIT Undergraduate of Mathematics.

9. Boneh, Dan and Matthew Franklin, July 2001. Efficient Generation of Shared RSA Keys. Journal of the ACM, Vol. 48, No. 4.
10. Yan, Song Y. 2004. Primality Testing and Integer Factorization in PublicKey Cryptography. Boston: Kluwer Academic Publishers.

Dimple Patel - dpatela@gmu.edu

1. <http://www2.toki.or.id/book/AlgDesignManual/BOOK/BOOK4/NODE143.HTM>
2. Reisel, Hans. Prime Numbers and Computer Methods for Factorization. 2nd ed.
3. Birkhauser. Boston. 1994. ISBN 0-8176-3743-5 and 3-7643-3743-5.
4. Ribenboim, Paulo. The New Book of Prime Number Records. 3rd ed.
5. Springer Verlag. New York 1996.
6. Cryptography and Network Security book chapters on Number theory
7. http://www-gap.dcs.st-and.ac.uk/~history/HistTopics/Prime_numbers.html
8. <http://216.239.41.104/search?q=cache:HOaPRK4LSv8J:www.grst.de/html/dsds/primegeneration.pdf+Generating+large+primes+for+cryptographic+applications&hl=en>
9. Handbook of Applied Cryptography, by A. Menezes, P. van Oorschot, and S. Vanstone, CRC Press, 1996, Chapter 4
10. paper:
http://www.ict.etsi.fr/eessi/documents/20011019_algorithm_proposal_V2.11.doc
11. <http://www.cse.iitk.ac.in/news/primality.pdf>
12. <http://grouper.ieee.org/groups/1363/Research/Web.html>

Robert Salembier - rsalembi@gmu.edu

1. Simple explanation of prime number:
http://www.campusprogram.com/reference/en/wikipedia/p/pr/prime_number.html
2. 3 simple prime number algorithms:
<http://www.olympus.net/personal/7seas/primes.html>
3. Basically describes prime number generation:
<http://mathforum.org/library/drmath/view/54317.html>

4. Applied Cryptography by Bruce Schneier (Chapt 11.4 Factoring, 11.5 Prime number generation, 19 Public-Key Algorithms, 19.3 RSA)
5. Handbook of Applied Cryptography by Arthur Menezes Chapt 4.4 Prime number generation
6. Code that generates prime number between 2 and whatever you say:
<http://www.planet-source-code.com/vb/scripts/ShowCode.asp?txtCodeId=8335&lngWId=3>
7. Tests for checking if number are prime:
<http://www.utm.edu/research/primes/prove/>
8. RSA Algorithm: http://www.di-mgt.com.au/rsa_alg.html
9. Public Key Algorithms:
<http://www.eskimo.com/~weidai/algorithms.html>
10. Random number generator: <http://www.betelgeuse-4.net/howto/random/index.php>

Paul Southerington - psouther@gmu.edu

1. Introductory Prime Number Theory Resources:
<http://www.maths.ex.ac.uk/~mwatkins/zeta/tutorial.htm>
2. Schneier, Bruce, Applied Cryptography
3. The Prime Pages: <http://www.utm.edu/research/primes/>
4. Mersenne Prime Search <http://www.mersenne.org/>
5. Bressoud, David M., Factorization and Primality Testing
6. Crandall & Pomerance, Prime Numbers
7. Menezes, Alfred et. al., Handbook of Applied Cryptography
8. "A Linear Sieve Algorithm For Finding Prime Numbers", Communications of the ACM, Vol 21, Issue 12, Dec. 1978
9. "Prime Sieves Using Binary Quadratic Forms", Atkin & Bernstein, Mathematics of Computation, #73 , pp.1023 - 1030, 2004
10. "Fast Generation of Prime Numbers and Secure Public-Key Cryptographic Parameters", Journal of Cryptology Vol. 8, No. 3, pp. 123-155, 1995

Clate Stansbury - clateiii@hotmail.com

1. PRIMES is in P, We present a deterministic polynomial-time algorithm that determines whether an input number n is prime or composite.
<http://www.cse.iitk.ac.in/news/primality.pdf>

2. Safe Prime Generation with a Combined Sieve, Michael J. Wiener, <http://eprint.iacr.org/2003/186.pdf>
3. Double-Speed Safe Prime Generation, David Naccache, <http://eprint.iacr.org/2003/175.pdf>
4. Efficient Computation Modulo a Shared Secret with Application to the Generation of Shared Safe-Prime Products, Joy Algesheimer and Jan Camenisch and Victor Shoup, <http://eprint.iacr.org/2002/029.pdf>
5. Finding primes & proving primality
 - <http://www.utm.edu/research/primes/prove/index.html>
 - <http://www.utm.edu/research/primes/prove/references.html>
 - <http://www.utm.edu/research/primes/notes/faq/>
6. The Three-Large_Primes Variant of the Number Field Sieve, Stefania Cavallar, <http://citeseer.ist.psu.edu/cache/papers/cs/26557/http:zSzzSzwww.cwi.nlzSzftpzSzCWIreportszSzMASzSzMAS-R0219.pdf/the-three-large-primes.pdf>
7. 41st Known Mersenne Prime Found!!, Includes faq, "how it works", executable, and source code for Mersenne, Prime Search software. <http://www.mersenne.org/>
8. Laboration 1: Large Numbers, <http://www.cs.umu.se/kurser/TDBC91/VT02/lab1.html>
9. Online Prime Number Tester and Browser, <http://www.prime-numbers.org/>

Harini Vasudevan - hvasudev@gmu.edu

1. <http://www.ssh.fi/support/cryptography/introduction>
2. <http://www.rsasecurity.com/rsalabs/node.asp?id=2158>
3. <http://www.experimentalstuff.com/Technologies/PDM/>
4. <http://bach.dynet.com/primes/>
5. <http://www-fs.informatik.uni-tuebingen.de/~reinhard/krypto/English/2.3.1.e.html>
6. http://www.gemplus.com/smart/r_d/publications/pdf/JPV00gen.pdf
7. <http://alas.matf.bg.ac.yu/~mr99067/matematika/navigator.php?strana=velprost&jezik=engli>
8. <shhttp://mathworld.wolfram.com/PrimeNumber.html>

9. <http://number-theory.math.designerz.com/number-theory-prime-numbers.php>
10. <http://www.maths.ex.ac.uk/~mwatkins/zeta/tutorial.htm>

Hybrid Software/Hardware Projects - Fall 2004

Cipher breaking

Factoring of large numbers using reconfigurable computer.

Miaoqing Huang - mqhuang@gwu.edu

1. <http://www.srccomputers.com/> The website of the manufacturer of platform
2. "SRC-6E MAP Hardware Guide", SRC Computers, Inc. 2004.
3. "SRC-6 C Programming Environment V1.7 Guide", SRC Computers, Inc. 2004.
4. Sashisu Bajracharya and Han Sang, "Comparison of Factorization Algorithms for Large Numbers - Project Specification", 2004
5. A.J.Menezes, P.C. Van Oorschot, and S.A.Vanstone, "Handbook of Applied Cryptology", Chapters 3.2.6-3.2.7, pp.95-98, 1997
6. "Factoring Large Numbers: Fun or Applied Science?", http://www.cwi.nl/publications/annualreports/1999/AR/PDF/factorin_g.pdf
7. Arjen K. Lenstra, Adi Shamir, Jim Tomlinson, Eran Tromer, "Analysis of Bernstein's Factorization Circuit", Proc. Asiacrypt 2002, LNCS 2501, 1-26, Springer-Verlag, 2002
8. Daniel J. Bernstein, "Circuits For Integer Factorization: A Proposal", NSF DMS, 2001
9. Adi Shamir, Eran Tromer, "On the cost of factoring RSA-1024", RSA CryptoBytes. Vol.6, No.2, 10-19, 2003
10. Arjen K. Lenstra, Adi Shamir, "Analysis and optimization of the TWINKLE factoring device", Proc. Euro-crypt 2002, LNCS 1807 35-52, Springer-Verlag, 2000

Dimple Patel - dpatela@gmu.edu

1. http://ece.gmu.edu/courses/ECE543/project/specs-F03/bajracharya_sang.pdf
2. <http://portal.acm.org/citation.cfm?id=508352.508353>
3. http://www.fact-index.com/i/in/integer_factorization.html
4. <http://www.fortunecity.com/emachines/e11/86/largeno.html>
5. http://cpe02.gmu.edu/rcm/publications/fidanci_RAW.pdf

6. <http://ipdps.eece.unm.edu/1998/raw/walrath.pdf>
7. <http://home.ecn.ab.ca/~jsavard/crypto/pk050204.htm>
8. http://216.239.39.104/search?q=cache:5JfROkjdXjEJ:www.cwi.nl/research/2001/TeRiele_Eng/TeRiele_E.pdf+factoring+of+large+numbers&hl=en
9. http://216.239.39.104/search?q=cache:frHeiYFCOCoJ:cpe02.gmu.edu/rcm/publications/FPT_2004.pdf+factoring+of+large+numbers+using+reconfigurable+computers&hl=en
10. white paper:
<http://216.239.39.104/search?q=cache:G8eJp8hOPeUJ:www.nallatech.com/solutions/applications/Documents/NT303-0006%2520RIPC%2520White%2520Paper.pdf+reconfigurable+computer+white+paper&hl=en>

New platforms for cryptography

Encryption and authentication of the FPGA bitstream.

Milind M. Parelkar - mparelka@gmu.edu

1. Applied Cryptography - Protocols, Algorithms and Source Codes in C, Bruce
2. Schneier, John Wiley and Sons, pp. 429 - One Way Hash Functions
3. K. Gaj, Lecture Slides for ECE 646 - Cryptography and Network Security, Lecture 12 (Fall 2003) - Hash Functions & MACs
3. Cryptography and Network Security: Principles and Practice, 3rd ed., William Stallings, Prentice Hall, pp. 311 - Message Authentication and Hash Functions
4. Is Your FPGA Design Secure? - XCell Journal Online, http://www.xilinx.com/publications/xcellonline/xcell_47/xc_secure47.htm
5. Security Scenarios <http://www.actel.com/documents/SecurityScenarios.pdf>
6. Design Security in Nonvolatile Flash and Antifuse FPGAs - www.actel.com/documents/DesignSecurity.pdf
7. T. Grembowski, R. Lien, K. Gaj, N. Nguyen, P. Bellows, J. Flidr, T. Lehman, B. Schott, "Comparative Analysis of the Hardware

- Implementations of Hash Functions SHA-1 and SHA-512" Proc.
Information Security Conference, Sao Paulo, Brazil
8. CipherStream Protocol—How CoolRunner-II CPLDs Protect FPGA,
Jesse Jenkins -
<http://direct.xilinx.com/bvdocs/whitepapers/wp197.pdf>
 9. FPGA implementation of SHA-1 Secure Hash standard, Roar Lien -
Master's Thesis, GMU
 10. A Whitepaper of SRAM FPGA Security, Ray Schouten -
http://www.fpga.com.cn/advance/skill/SRAM_Security_whitepaper.pdf

Hardware Projects - Fall 2004

Secret-key cryptosystems

Implementation of a selected secret-key cipher optimized for the minimum area and power.

Curtis Christian - cchrist4@gmu.edu

1. Stallings, William. Cryptography and Network Security. New Jersey: Pearson Education, 2003, Chapters 3,6
2. Menezes, A. van Oorschot, P. and Vanstone, S. Handbook of Applied Cryptography. CRC Press, 1996. Chapter 7, (see also, <http://www.cacr.math.uwaterloo.ca/hac>)
3. Schneier, Bruce. Applied Cryptography. John Wiley & Sons, 1996, Chapters 12-15.
4. Steve Trimberger¹, Raymond Pang, and Amit Singh, "A 12 Gbps DES Encryptor/Decryptor Core in an FPGA", Ç.K. Koç and C. Paar (Eds.): CHES 2000, LNCS 1965, pp. 156 - 163, 2000. © Springer-Verlag Berlin Heidelberg 2000
5. Jens-Peter Kaps and Christof Paar, "Fast DES Implementations for FPGAs and Its Application to a Universal Key-Search Machine", S. Tavares and H. Meijer (Eds.): SAC'98, LNCS 1556, pp. 234{247, 1999.© Springer-Verlag Berlin Heidelberg 1999
6. Allen Michalski, Kris Gaj, and Tarek El-Ghazawi, "An Implementation Comparison of an IDEA Encryption Cryptosystem on Two General-Purpose Reconfigurable Computers" P.Y.K. Cheung et al. (Eds.): FPL 2003, LNCS 2778, pp. 204-219, 2003. © Springer-Verlag Berlin Heidelberg 2003
7. Pawel Chodowiec and Kris Gaj, "Very Compact FPGA Implementation of the AES Algorithm" C.D. Walter et al. (Eds.): CHES 2003, LNCS 2779, pp. 319-333, 2003. © Springer-Verlag Berlin Heidelberg 2003
8. Alireza Hodjat and Ingrid Verbauwhed, "A 21.54 Gbits/s Fully Pipelined AES Processor on FPGA"
9. Guido Bertoni, Luca Breveglieri, Pasqualina Fragneto, Marco Macchetti, and Stefano Marchesin, "Efficient Software Implementation of AES on 32-Bit Platforms", B.S. Kaliski Jr. et al. (Eds.): CHES 2002, LNCS 2523, pp. 159-171, 2003. © Springer-Verlag Berlin Heidelberg 2003

10. Sean Murphy and Matthew J.B. Robshaw, "Essential Algebraic Structure within the AES", M. Yung (Ed.): CRYPTO 2002, LNCS 2442, pp. 1-16, 2002. © Springer-Verlag Berlin Heidelberg 2002
11. Johannes Wolkerstorfer, Elisabeth Oswald, and Mario Lamberger, "An ASIC Implementation of the AES SBoxes", B. Preneel (Ed.): CT-RSA 2002, LNCS 2271, pp. 67-78, 2002. © Springer-Verlag Berlin Heidelberg 2002
12. Akashi Satoh and Sumio Morioka, "Hardware-Focused Performance Comparison for the Standard Block Ciphers AES, Camellia, and Triple-DES", C. Boyd and W. Mao (Eds.): ISC 2003, LNCS 2851, pp. 252-266, 2003. © Springer-Verlag Berlin Heidelberg 2003
13. Cameron Patterson, "A Dynamic FPGA Implementation of the Serpent Block Cipher", K. Ko and C. Paar (Eds.): CHES 2000, LNCS 1965, pp. 141-155, 2000. © Springer-Verlag Berlin Heidelberg 2000
14. Gael Rouvroy, Francois-Xavier Standaert, Jean-Jacques Quisquater, and Jean-Didier Legat, "Design Strategies and Modified Descriptions to Optimize Cipher FPGA Implementations: Fast and Compact Results for DES and Triple-DES", P.Y.K. Cheung et al. (Eds.): FPL 2003, LNCS 2778, pp. 181-193, 2003. © Springer-Verlag Berlin Heidelberg 2003
15. François Charot, Eslam Yahya, and Charles Wagner, "Efficient Modular-Pipelined AES Implementation in Counter Mode on ALTERA FPGA", P.Y.K. Cheung et al. (Eds.): FPL 2003, LNCS 2778, pp. 282-291, 2003. © Springer-Verlag Berlin Heidelberg 2003
16. Jean-Luc Beuchat, "FPGA Implementations of the RC6 Block Cipher", P.Y.K. Cheung et al. (Eds.): FPL 2003, LNCS 2778, pp. 101-110, 2003. © Springer-Verlag Berlin Heidelberg 2003
17. Nazar A. Saqib, Francisco Rodríguez-Henríquez, and Arturo Díaz-Pérez, "Two Approaches for a Single-Chip FPGA Implementation of an Encryptor/Decryptor AES Core", P.Y.K. Cheung et al. (Eds.): FPL 2003, LNCS 2778, pp. 303-312, 2003. © Springer-Verlag Berlin Heidelberg 2003
18. G.P. Saggese¹, A. Mazzeo¹, N. Mazzocca², and A.G.M. Strollo¹, "An FPGA-Based Performance Analysis of the Unrolling, Tiling, and Pipelining of the AES Algorithm", P.Y.K. Cheung et al. (Eds.): FPL 2003, LNCS 2778, pp. 292-302, 2003. © Springer-Verlag Berlin Heidelberg 2003
19. Kris Gaj and Pawel Chodowiec, "Fast Implementation and Fair Comparison of the Final Candidates for Advanced Encryption Standard

- Using Field Programmable Gate Arrays", D. Naccache (Ed.): CT-RSA 2001, LNCS 2020, pp. 84-99, 2001. © Springer-Verlag Berlin Heidelberg 2001
20. Pawel Chodowiec, Kris Gaj, Peter Bellows, and Brian Schott, "Experimental Testing of the Gigabit IPsec-Compliant Implementations of Rijndael and Triple DES Using SLAAC-1V FPGA Accelerator Board", G.I. Davida and Y. Frankel (Eds.): ISC 2001, LNCS 2200, pp. 220-234, 2001. © Springer-Verlag Berlin Heidelberg 2001
 21. Kazumaro Aoki, Tetsuya Ichikawa, Masayuki Kanda, Mitsuru Matsui, Shiho Moriai, Junko Nakajima, Toshio Tokita, "Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms"
 22. Akashi Satoh and Sumio Morioka, "Unified Hardware Architecture for 128-Bit Block Ciphers AES and Camellia", C.D. Walter et al. (Eds.): CHES 2003, LNCS 2779, pp. 304-318, 2003. © Springer-Verlag Berlin Heidelberg 2003
 23. Tsung-Fu Lin, Chih-Pin Su, Chih-Tsun Huang, and Cheng-Wen Wu, "A High-Throughput Low-Cost AES Cipher Chip"
 24. Alireza Hodjat, Patrick Schaumont, Ingrid Verbauwhede, "Architectural Design Features of a Programmable High Throughput AES Coprocessor",
 25. Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04) 0-7695-2108-8/04 © 2004 IEEE
 26. Henry Kuo, Ingrid Verbauwhede, "Architectural Optimization for a 1.82Gbits/sec VLSI Implementation of the AES Rijndael Algorithm"
 27. AES candidate VHDL source code and test benches, NIST, 2000

Porting NSA VHDL codes and other public domain codes to Field Programmable Gate Arrays.

Ron Sulpizio - rsulpizi@gmu.edu

1. Associated Professional Systems, FPGA Basics.
<http://users.erols.com/aaps/x84lab/FPGA.html>

2. Kean, Tom, Cryptographic Rights Management of FPGA Intellectual Property Cores, February 2002.
<http://www.algotronix.com/content/security%20fpga2002.pdf>
3. NIST, Round 2 Analysis, November 27, 2000.
<http://csrc.nist.gov/CryptoToolkit/aes/round2/r2anlsys.htm>
4. McDaniel, Larry T., III, An Investigation of Differential Power Analysis Attacks on FPGA-based Encryption Systems -- Thesis submitted to the Faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the degree of Master of Science in Electrical Engineering, May 29, 2003.
http://scholar.lib.vt.edu/theses/available/etd-06062003-163826/unrestricted/Larry_McDaniel.pdf
6. Beuchat, Jean-Luc, FPGA Implementations of the RC6 Block Cipher, 2003. <http://perso.ens-lyon.fr/jean-luc.beuchat/Publications/fpl2003.pdf>
7. Chodowiec, Pawel R., Comparison of the Hardware Performance of AES Candidates Using Reconfigurable Hardware, 2002.
http://ece.gmu.edu/reports/Pawel_Chodowiec_MS_Thesis.pdf
8. Weaver, Nicholas C., A High Performance, Compact Rijndael (AES) Core for the Virtex Family FPGA, March 6, 2002.
<http://www.cs.berkeley.edu/~nweaver/rijndael/>
9. Chodowiec, Pawel, et al., Implementation of the Twofish Cipher Using FPGA Devices, July 1999. <http://www.schneier.com/paper-twofish-fpga.pdf>
10. Paar, Christof, et al., An Algorithm-Agile Cryptographic Co-processor Based on FPGAs, September 20, 1999. <http://www.crypto.ruhr-uni-bochum.de/imperia/md/content/texte/brendonpaarspie99.pdf>
11. Helion, High Performance Solutions in Silicon, website.
<http://www.heliontech.com/core.htm>

Public key cryptosystems

Implementation of a selected public key algorithm based on modular exponentiation (RSA, DSA, D-H).

Ron Sulpizio - rsulpizi@gmu.edu

1. Kessler, Gary C. An Overview of Cryptography, May 1998.
<http://www.garykessler.net/library/crypto.html>
2. Electronic News, Altera Confirms Guidance, Rolls Out Reusable Core, September, 2003. <http://www.reed-electronics.com/electronicnews/article/CA320671?pubdate=08%2F31%2F2003>
3. Telikepalli, Anil, et al., Is Your FPGA Design Secure?, May 2003.
http://www.xilinx.com/publications/xcellonline/xcell_47/xc_secure47.htm
4. Shihab, Ahmed, et al., Implementing IKE Capabilities in FPGA Designs, December 2003.
<http://www.commsdesign.com/showArticle.jhtml?articleID=16600061>
5. Khaldoun, M., Prototyping of Scalable Montgomery Multiplier using Field Programmable Gate Arrays (FPGAs), 2002.
<http://security.ece.orst.edu/papers/O2Khaldoun.html>
6. Fry, John, et al., FPGAs Lower Costs for RSA Cryptography, September 26, 2003.
http://www.eet.com/in_focus/mixed_signals/OEG20030926S0022
7. Chinuk, Kim, VHDL Implementation of Systolic Modular Multiplications on RSA Cryptosystem, January 2001. http://www-cs.engr.cuny.cuny.edu/~gertner/Students/Master/Chinuk/MS_Thesis_Chinuk_Kim.PDF
8. Ciet, Mathieu, et al., Parallel FPGA Implementation of RSA with Residue Number Systems,
<http://www.dice.ucl.ac.be/crypto/index.php?page=pdf162.pdf>
9. Helion, High Performance Solutions in Silicon -- Fast RSA core.
<http://www.heliontech.com/core.htm>
10. Mazzeo, A., et al., FPGA-based Implementation of a serial RSA Processor, 2003.
http://sigda.org/Archives/ProceedingArchives/Date/papers/2003/datte03/pdffiles/07b_3.pdf

Implementation of an emerging public key cryptosystem NTRU using FPGA devices.

Curtis Christian - cchrist4@gmu.edu

1. Baily, Daniel. "NTRU: Technical Overview and Applications", NTRU Cryptosystems, Inc.
2. NTRU Cryptosystems, Inc, "The NTRU Public Key Cryptosystem - A Tutorial", web site: www.ntru.com/cryptolab/tutorials.htm
3. "More Public Key Cryptography", lecture notes currently of unknown origin, which I need to retrace
4. NTRU: A Ring Based Public Key Cryptosystem, Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman, in Algorithmic Number Theory (ANTS III), Portland, OR, June 1998, J.P. Buhler (ed.), Lecture Notes in Computer Science 1423, © Springer-Verlag, Berlin, 1998, 267-288.
5. Jeffrey Hoffstein, Joseph Silverman, "Random Small Hamming Weight Products with Applications to Cryptography", technical report, NTRU Cryptosystems
6. "Lattices in Cryptography", parts I and II, lecture notes currently of unknown origin, which I need to retrace
7. Gross, Greg. "Truncated Polynomials in the NTRU Cryptosystem", NTRU Cryptosystems, Inc., May 6, 2002
8. O'Rourke, Colleen Marie. "Efficient NTRU Implementations", Masters Thesis, Worcester Polytechnic Institute, April 2002
9. Lenstra, Arjen K. "Computational Methods in Public Key Cryptology", Citibank, N.A., August 14, 2002
10. Greg Gross, "Truncated Polynomials in the NTRU Cryptosystem", technical report, NTRU Cryptosystems, May 2002
11. Joseph Silverman, "High-speed Multiplication of (Truncated) Polynomials", technical report, NTRU Cryptosystems, January 1999
12. Jeffrey Hoffstein, Joseph Silverman, "Optimizations for NTRU", technical report, NTRU Cryptosystems

Analytical Projects - Fall 2004

Implementations of cryptosystems

Comparison of the ASIC-, FPGA-, and microprocessor-based implementations of cryptographic algorithms and protocols.

Ganeshprasad Maddipati - gmaddipa@gmu.edu

1. scholar.lib.vt.edu/theses/available/etd-06122003-153755/unrestricted/harper_dissertation_etd.pdf
2. www.iaik.tu-graz.ac.at/research/publications/theses/schindler.pdf
3. ieee.uwaterloo.ca/fydp/projects2001.html
4. www.cse.cuhk.edu.hk/~phwl/papers/rccrypto.ppt
5. www.cise.ufl.edu/~jabellad/NP.dochttp://csdl.computer.org/comp/proceedings/fccm/2003/1979/00/19790292.pdf
6. <http://lotus1000.usc.edu/prasanna/papers/dandalisOSEE00.pdf>
7. <http://www.crypto.ruhr-uni-bochum.de/imperia/md/content/texte/brendonpaarspie99.pdf>
8. <http://lotus1000.usc.edu/prasanna/papers/dandalisFCCM00.pdf>
9. http://ece.gmu.edu/crypto/kgaj_2002_10_isc.pdf
10. <http://www.ece.wpi.edu/Research/Crypt/Publications/Documents/aelbirtpaarieeetranvlsi.pdf>
11. <http://www.discretix.com/PDF/Security%20Implications%20of%20Hardware%20vs.%20Software%20Cryptographic%20Modules.pdf>
12. <http://www.mit.edu/~chuvpilo/papers/chuvpilo-2002-LCS.pdf>
13. <http://islab.oregonstate.edu/koc/ece679/project/2003/park.pdf>
14. http://www.agere.com/telecom/docs/building_new.pdf
15. http://www.agere.com/telecom/nps_whitepapers.html
16. www.cavium.com/pdfFiles/NITROX-PB-SSL-1.3.pdf
17. <http://csrc.nist.gov/CryptoToolkit/aes/round2/conf3/papers/23-adandalis.pdf>
18. www.cypherpunks.to/~peter/usenix00.pdf
19. delta.cs.cinvestav.mx/~adias/RecComp2003/SemFPGA.pdf
20. www.crypto.ruhr-uni-bochum.de/imperia/md/content/texte/wollinger_howsecurearefpgasincryptoapp_longversion.pdf
21. <https://www.cosic.esat.kuleuven.ac.be/publications/article-26.pdf>

22. eee.ucc.ie/staff/marnanel/Files/papers/McIvor_Asilomar2003.pdf
23. www.smartcard.co.uk/resources/tutorials/sct-scail.pdf

Survey of the commercially available chips and IP cores implementing cryptographic algorithms.

Miaoqing Huang - mghuang@gwu.edu

1. <http://www.cavium.com/> The website of Cavium, provider of many security chips
2. <http://www.rsasecurity.com/> RSA Security Inc. is another major security chips maker
3. http://www.broadcom.com/products/category.php?category_id=25
The web pages listing the security processors provided by Broadcom
4. <http://www.safenet-inc.com/> The website of SafeNet
5. "Intel IXP 2850 Network Processor Specification", Intel Corporation, 2004
6. <http://www.hifn.com/products/Security.html> Security Products page of HiFn Company
7. <http://www.corrent.com/> The website of Corrent Company
8. <http://www.aepsystems.com/> The website of AEP Systems
9. <https://www.netcontinuum.com/products/index.cfm> The website of Netcontinuum
10. <http://www.netoctave.com/netoctave.asp?template=products> The products pages of Netoctave Company

Comparative analysis of existing academic and commercial implementations of AES in hardware.

Comparative analysis of existing academic and commercial implementations of AES in software.

Tom Saunders - iamsaunders@netscape.net

1. <http://palms.ee.princeton.edu/PALMSopen/fiskiran00performance-pres.pdf> limited information but very technical
2. <http://mirrors.isc.org/pub/www.watersprings.org/pub/id/draft-irtf-cfrg-cwc-01.txt>, Crypto Forum Research Group T. Kohno Internet-Draft UC San Diego ...
3. <http://kingkong.me.berkeley.edu/~kenneth/courses/sims250/des.html>
4. <http://www.macfergus.com/pub/AESperformance.pdf>
5. <http://islab.oregonstate.edu/koc/ece679/project/2003/thiagarajan-gourishetty.pdf>, Study of AES and its Efficient Software Implementation
6. <http://www.crypto.ruhr-uni-bochum.de/imperia/md/content/texte/wollingeretalaes3.pdf>, How Well Are High-End DSPs Suited for the AES Algorithms?
7. <http://www.cercs.gatech.edu/tech-reports/tr2004/git-cercs-04-27.pdf>, High Speed Memory Centric Protection on Software Execution Using ...
8. <http://www.eecs.umich.edu/~taustin/papers/ISPASS01-gpvlong.pdf>, Performance Analysis Using Pipeline Visualization
9. <http://th.informatik.uni-mannheim.de/people/lucks/papers/helix.pdf>. Fast Encryption and Authentication in a Single Cryptographic Primitive
10. <http://www.schneier.com/paper-fast-software-encryption.pdf>, Fast Software Encryption: Designing Encryption Algorithms for ...

Cryptographic capabilities of Network Processors.

Usman Akhtar - uakhtar@gmu.edu

1. <http://portal.acm.org/citation.cfm>: Network Processing in Content Inspection Applications.
2. <http://csdl.computer.org>: Software Processing Performance in Network Processors.
3. <http://www.cs.berkeley.edu>: understanding of NPs
4. <http://csdl.computer.org>: Utilizing Formal Assertions for System Design of Network Processors
5. <http://portal.acm.org/citation.cfm>: Challenges and Opportunities in Broadband and Wireless Communication Designs.

6. [http:// portal.acm.org/citation.cfm](http://portal.acm.org/citation.cfm): Challenges and Opportunities in Broadband and Wireless Communication Designs
7. <http://www.intel.com>:Innovations in Network Processors
8. <http:// portal.acm.org/citation.cfm>: The Basics of Network Processors
9. <http:// portal.acm.org/citation.cfm>: Net processor book ties architectures to applications
10. <http:// portal.acm.org/citation.cfm>: Network chips gear up for better security, services; Network Processors Conference showcases array of new processors
11. <http://www.m2.com>: Hewlett-Packard ships new HP Atalla Network Security Processors.
12. http://mutex.gmu.edu:2147/pdfserve/get_item/1/S31cd8ew62/SB886_02.pdf

Aparna Kasturi - akasturi@gmu.edu

1. Computer security, Art and Science --Matt Bishop Addison-Wesley 2003
2. C.P.Pfleeger and S.L.Pfleeger, Security in Computing, 3rd ed, Prentice Hall 2003
3. http://www.eetimes.com/article/printableArticle.jhtml?articleID=16505932&url_prefix=in_focus/communications&sub_taxonomyID=
4. http://www.wordiq.com/definition/Computer_security
5. <http://encyclopedia.thefreedictionary.com/Computer%20security>
6. <http://www.cc.gatech.edu/gvu/people/Phd/Ian/coocs-95.html>
7. <http://www.erights.org/elib/capability/ode/ode-protocol.html>
8. http://www.3gpp2.org/Public_html/specs/S.R0082-0_v1.0_110703.pdf
9. http://www.snia.org/data/resources/presentations/19980922_Presentations/19981001_Network_Attached_Secure_Dis.pdf
10. http://scholar.lib.vt.edu/theses/available/etd-06122003-153755/unrestricted/harper_dissertation_etd.pdf

Uma Koppula - ukoppula@gmu.edu

1. <http://www.netrino.com/Articles/NetworkProcessors/>
2. A Guide to Security and Content Processors, Third Edition Authors: Sanjay Iyer and Linley Gwennap
3. http://www.intel.com/technology/itj/2002/volume06issue03/art02_security/p03_secarchitecture.htm
4. <http://www.futsoft.com/pdf/NPwp.pdf>
5. Network Systems Design Using Network Processors by Douglas E. Comer
6. Network Processor Design : Issues and Practices, Volume 2 by Patrick Crowley, Mark A. Franklin, Haldun Hadimioglu, Pater Z. Onufryk
7. http://www.eetimes.com/article/printableArticle.jhtml?articleID=16505932&url_prefix=in_focus/communications&sub_taxonomyID=
8. <http://www.cs.ucr.edu/~bhuyan/papers/np1.pdf>
9. <http://www.ecs.umass.edu/ece/wolf/papers/wwc2003.pdf>
10. http://ceaspub.eas.asu.edu/Ye_Activities/515, 20, Future Plans (Y2)

Ganeshprasad Maddipati - gmaddipa@gmu.edu

1. www.roke.co.uk/download/white_papers/network_processors_introduction.pdf
2. <http://www.cs.berkeley.edu/~culler/cs252-s02/slides/lec14-netproc.pdf>
3. www.cs.ucr.edu/~bhuyan/cs162/LECTURE9.ppt
4. www.cs.ucr.edu/~bhuyan/CS213/2004/LECTURE7.ppt
5. www.cise.ufl.edu/~jbellad/NP.doc
6. dinki.mine.nu/weblog/b2-img/arch.ppt
7. http://www.lightreading.com/document.asp?doc_id=19354
8. <http://www.commsdesign.com/main/2000/07/0007feat3.htm>
9. lhcb-comp.web.cern.ch/lhcb-comp/DAQ/Talks/Introduction%20to%20Network%20Processors.ppt
10. lhcb-comp.web.cern.ch/lhcb-comp/DAQ/Talks/Implementation-stripped.ppt
11. http://www.stork.eu.org/papers/25_future_of_cryptoimplementation.pdf
12. <http://netlab.cs.tsinghua.edu.cn/~ljsheng/npu/>
13. www.ecs.umass.edu/ece/wolf/courses/ECE697J/Fall2002/presentations/ECE697J-02-11-12.pdf
14. http://homepage.mac.com/macdomeeu/lu/Modern_Cryptography.pdf

15. <http://www.ecs.umass.edu/ece/wolf/papers/wwc2003.pdf>
16. <http://www.discretix.com/PDF/Security%20Implications%20of%20Hardware%20vs.%20Software%20Cryptographic%20Modules.pdf>
17. http://www.hbarel.com/publications/Security_Implications_of_HW_vs_SW_Cryptographic_Modules.pdf
18. <http://ocw.mit.edu/NR/rdonlyres/Electrical-Engineering-and-Computer-Science/6-823Computer-System-ArchitectureSpring2002/91150BC6-E5E5-4092-9A71-D03821765E3A/0/lecture24.pdf>
19. http://www.roke.co.uk/networks/hardware/network_processors.asp
20. http://www-106.ibm.com/developerworks/eserver/articles/java_hardware.html
21. <http://www.cs.ucr.edu/~bhuyan/papers/np1.pdf>
22. http://www.agere.com/telecom/docs/building_new.pdf
23. http://www.agere.com/telecom/docs/challenge_new.pdf
24. www-dse.doc.ic.ac.uk/Events/opensig-2001/droz.pdf
25. www.networksystemsdesign.com/English/Collaterals/Newsletters/2002/Newsletter_200208.pdf

Tarun Nallabelli - tnallabe@gmu.edu

1. <http://www.embedded.com/showArticle.jhtml?articleID=26806189>
2. <http://www.networkmagazineindia.com/200107/process1.htm>
3. <http://www.ezchip.com/images/pdfs/EZchip%20security%20whpaper%20v1.0.pdf>
4. http://www.lightreading.com/document.asp?doc_id=19354
5. <http://www.commsdesign.com/main/2000/07/0007feat3.htm>
6. http://www.intel.com/technology/itj/2002/volume06issue03/art02_security/p01_abstract.htm
7. <http://www.cs.ucr.edu/~bhuyan/papers/np1.pdf>
8. Design-space exploration of the most widely used cryptography algorithms • ARTICLE Microprocessors and Microsystems, In Press, Uncorrected Proof, Available online 11 September 2004, I. Papaefstathiou, V. Papaefstathiou and C. Sotiriou, http://www.sciencedirect.com/science?_ob=ArticleURL&_aset=B-WA-A-B-EE-MSAYVW-UUA-AUEYBEABBE-AUECEDWABE-ZBBBBAUWA-EE-U&_rdoc=2&_fmt=full&_udi=B6VOX-4D97GSH-4&_coverDate=09%2F11%2F2004&_cdi=5658&_orig=search&_st=13&

- [_sort=d&view=c&_acct=C000035118&_version=1&_urlVersion=0&_use
rid=650615&md5=8d04cf57f9c14c0274682b83e0d41bf5](#)
9. <http://www.cs.berkeley.edu/~plishker/UnderstandingNPs.pdf>
 10. [http://www.intel.com/technology/itj/2002/volume06issue03/vol6iss3
_networkprocessors.pdf](http://www.intel.com/technology/itj/2002/volume06issue03/vol6iss3
_networkprocessors.pdf)

Swethana Pagadala - spagadal@gmu.edu

1. Guide to Network Processors(fifth edition book)-Authors: Bob Wheeler and Linley Gwennap.
2. Guide to Access Processors(first edition book)-Authors: Sanjay Iyer and Jag Bolaria.
3. Introduction to Network Processors-paper by Mark Kohler.
4. High Integration makes IP Security fly- paper from EETIMES-The Industry for Engineers and Technical managers worldwide.
5. Capability-based Financial Instruments-paper presented at Financial Cryptography 2000
 - Mark S. Miller, ERights.org
 - Chip Morningstar, Communities.org
 - Bill Frantz,Communities.org
6. Innovations in Network Processors -Intel Technology Journal, Volume 6 Issue 3, August 2002 - by Jim Finnegan ,Co-General Manager, Network Processor Division, Intel Communications Group.
7. CommsDesign-Building TCP proxies for layers 5 to 7-Oscar R.Mitchell and Rick Hall.
8. Network Attached Secure Disks(NASD)-by Bill Courtright -Carnegie Mellon University.
9. Network Processors:balancing higher performance versus better security - by Misha Nossik.
10. Encryption-based protection for interactive user/computer communication-paper by Stephen Kent.

Sheryl Pinto - spinto@gmu.edu

1. <http://www.eetimes.com/story/OEG20020419S0080>

2. http://www.xilinx-china.com/esp/wired/optical/xlnx_net/net_proc.htm
3. <http://www.cs.ucsd.edu/~w2zhang/CSE237/>
4. <http://www.elecdesign.com/Articles/Index.cfm?ArticleID=3067&pg=3>
5. Network Processors. (2002, August 08). [Online]. Available: http://www.lightreading.com/document.asp?site=lightreading&doc_id=19354&page_number=1
6. Architectural Analysis of Cryptographic Applications for Network Processors Haiyong Xie, Li Zhou, and Laxmi Bhuyan Department of Computer Science & Engineering University of California, Riverside
7. Feghali, W., Burres, B., Wolrich, G., Carrigan, D., "Security: Adding Protection to the Network via the Network Processor." Intel Technology Journal

Tom Saunders - iamsaunders@netscape.net

1. <http://www.cs.ucsd.edu/~w2zhang/CSE237/>
2. <http://developer.novell.com/research/appnotes/1997/november/01/05.htm>, New issues in n/w security
3. http://www-cad.eecs.berkeley.edu/~mescal/presentations/networks_ipsoc2001.pdf touches on many issues including security
4. http://www.xilinx.com/esp/wired/optical/xlnx_net/net_proc.htm, not much data but many links
5. Hodjat and I. Verbaauwhede, "High-throughput programmable cryptocoprocessor," IEEE Micro Magazine May/June 2004.
6. http://www.ezchip.com/html/tech_security.html, EZchip Network Processors - Security Architectures White Paper
7. www.cs.berkeley.edu/~plishker/UnderstandingNPs.pdf, Understanding network processors
8. <http://www.cse.seas.wustl.edu/techreportfiles/getreport.asp?313>, Pipeline Task Scheduling on Network Processors 1 Introduction
9. http://www.cs.wpi.edu/~rek/Adv_Nets/Summer2003/SAN.pdf, Storage Area Networks: Performance and Security
10. <http://www.cs.ucr.edu/~bhuyan/papers/np1.pdf>, Architectural Analysis of Cryptographic Applications for Network processors

Key management

Survey of software packages supporting Public Key Infrastructure.

Mayur Enjamoori - menjamoo@gmu.edu

1. http://www.keylogger-online-detective.com/Security-kl/Public_Key_Infrastructure-kl/index.php
2. <http://www.ealaddin.com/hasp/default.asp>
3. <http://www.ealaddin.com/etoken/default.asp>
4. <http://www.deltacrypt.com/english/technology/pki.htm>
5. <http://www.finallysoftware.com/>
6. <http://whitepapers.zdnet.co.uk/0,39025945,60024364p-39000416q,00.htm>
7. <http://www.europpeki.org/php/home.php>
8. http://www.soltrus.com/english/corporate/pr_pkimodern_102003.htm
9. http://www.securitybox.net/eng/product/sbox_business.html

Rohan Misquith - rmisquit@gmu.edu

1. <http://ospkibook.sourceforge.net/docs/OSPki-2.4.7/OSPki-html/ospki-book.htm>
2. Understanding the Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations by Steve Lloyd, Carlisle Adams
3. <http://en.wikipedia.org/wiki/PKI>
4. http://internet.about.com/library/aa_pki1_082702.htm
5. www.cs.dartmouth.edu/~pki02/Thompson/slides.ppt intro
6. <http://www.computel.com.lb/Downloads/PKI.pdf>
7. <http://www.articsoft.com/index.htm>
8. http://www.keylogger-online-detective.com/Security-kl/Public_Key_Infrastructure-kl/index.php
9. <http://www.iosoftware.com/pages/Support/PKI/index.asp>
10. http://knowledgestorm.inc.com/search/index/inc/sol_summary/65538
11. <http://www.eldos.org/pkitools/pkitools.html>

12. <http://www.cryptomathic.dk/company/index.html>

Srikanth Nannapaneni - snannapa@gmu.edu

1. <http://www.cs.auckland.ac.nz/~pgut001/pubs/pkitutorial.pdf>
2. http://publib.boulder.ibm.com/infocenter/pseries/index.jsp?topic=/com.ibm.aix.doc/aixbman/security/cas_pki.htm
3. <http://security.ittoolbox.com/browse.asp?c=SecurityPeerPublishing&r=%2Fpub%2FSM031702e%2Epdf>
4. http://www.au-kbc.org/bpmain1/PKI/Trustpoint_PKI.pdf
5. <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:d04157.pdf> status of federal public key infrastructure activities at major federal departments and agencies : report to the Committee on Government Reform and the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, House of Representatives.
6. Understanding PKI: Concepts, Standards, and Deployment Considerations, Second Edition by Carlisle Adams, Steve Lloyd
7. PKI: Implementing & Managing E-Security by Andrew Nash, Bill Duane, Derek Brink, Celia Joseph
8. PKI : A Wiley Tech Brief by Tom Austin
9. PKI : implementing and managing E-security by Andrew Nash.
10. Planning for PKI : best practices guide for deploying public key infrastructure by Russ Housley, Tim Polk

Rajesh Ravi - rravi@gmu.edu

1. About public Key Infrastructure:
<http://www.opengroup.org/public/tech/security/pki/>
2. The PKI page: <http://www.pki-page.org/>
3. PKI documents: <http://csrc.nist.gov/pki/documents/welcome.html>
4. Deltacrypt Encryption software :
<http://www.deltacrypt.com/english/technology/pki.htm>
5. Website: <http://www.ealaddin.com/hasp/default.asp>
6. Europe PKI: <http://www.europempi.org/php/background.php>
7. PKI forum: <http://www.pkiforum.org/>

8. Website: <http://whitepapers.zdnet.co.uk/0,39025945,60024364p-39000416q,00.htm>
9. Website: <http://www.europepki.org/php/home.php>
10. Website: http://www.keylogger-online-detective.com/Security-kl/Public_Key_Infrastructure-kl/index.php Report on commercial Certification Authorities.

Report on Commercial Certification Authorities

Zonayed Faruque - zonayed@gmail.com

1. AlphaTrust.com (<http://www.alphatrust.com>)
2. eOriginal, Inc. (<http://www.das-inc.com/>)
3. Entegriety Solutions Corporation (Certification Products and Services) (<http://www.entegriety.com/>)
4. Equifax Secure, Inc. (<http://www.equifaxsecure.com/ebusinessid/>)
5. GTE Cybertrust (Certification Products) (<http://www.cybertrust.com/>)
6. IBM World Registry ([\http://www.internet.ibm.com/commercepoint/registry/index.html](http://www.internet.ibm.com/commercepoint/registry/index.html))
7. MIT Internet PCA Registration Authority
8. PenOP - Signature Dynamics Authentication Technology (<http://bs.mit.edu:8001/ipra.html>)
9. Utah Digital Signature Program and Licensed CAs and Repositories: (<http://www.commerce.state.ut.us/digsig/dsmain.htm>)
10. Digital Signature Trust Company (<http://www.digsigtrust.com/>)
11. Universal Secured Encryption Repository Company (USERFirst) (<http://www.usertrust.com/>)
12. The Usertrust Network (<http://www.usertrust.com/>)
13. Verisign (<http://www.verisign.com/>)
14. SET Certificate Authority (<http://www.setco.org/certificate.html>)
15. SUN Certification Authorities (<http://www.sun.com/security/product/ca.html>)
16. TradeWave Corporation (<http://www.tradewave.com/>)
17. Utah Digital Signature Authority (<http://www.tradewave.com/>)

18. Valicert (Complementary service to CAs)
(<http://www.tumbleweed.com/>)
19. Verisign (<http://www.verisign.com/>)
20. Washington Electronic Authentication Web Site
(<http://www.secstate.wa.gov/ea/>)
21. IDCertify (<http://www.idcertify.com/>)

Implementations of security protocols

Secure e-mail. Analysis of existing implementations of S/MIME.

Jon Halperin- jmhalper@cox.net

Aparna Kasturi - akasturi@gmu.edu

1. <http://www.infosyssec.org/infosyssec/hotlinks3.htm>
2. <http://csrc.nist.gov/publications/nistpubs/800-49/sp800-49.pdf>
3. <http://www.cs.auckland.ac.nz/~pgut001/links/books.html>
4. <http://www.itsecurity.com/papers/lacunae1.htm>
5. http://www.comms.scitech.susx.ac.uk/fft/crypto/sign_encrypt7.pdf
6. <http://info.aanekoski.fi/~mpe/suojaus/laws.html>

Tarun Nallabelli - tnallabe@gmu.edu

1. Safe email, safe office, and safe web browser demo description, Balzer, R.; DARPA Information Survivability Conference and Exposition, 2003. Proceedings , Volume: 2 , 22-24 April 2003 Pages:116 vol.2, <http://ieeexplore.ieee.org/iel5/8503/26876/01194941.pdf?tp=&arnumber=1194941&isnumber=26876&arSt=116%20vol.2&ared=&arAuthor=Balzer%2C+R.%3B>
2. Formal development of secure email, Dan Zhou; Kuo, J.C.; Older, S.; Chin, S.K.; System Sciences, 1999. HICSS-32. Proceedings of the 32nd Annual Hawaii International Conference on , Volume: Track3 , 5-8 Jan. 1999 Pages:10 pp. <http://ieeexplore.ieee.org/iel5/6293/16783/00772903.pdf?tp=&arnu>

- [mber=772903&isnumber=16783&arSt=10%20pp.&ared=&arAuthor=Da
n+Zhou%3B+Kuo%2C+J.C.%3B+Older%2C+S.%3B+Chin%2C+S.K.%3B](#)
3. Certified exchange of electronic mail (CEEM), Al-Hammadi, B.;
Shahsavari, M.; Southeastcon '99. Proceedings. IEEE , 25-28 March
1999 Pages:40 - 43,
[http://ieeexplore.ieee.org/iel5/6211/16590/00766087.pdf?tp=&arnu
mber=766087&isnumber=16590&arSt=40&ared=43&arAuthor=Al-
Hammadi%2C+B.%3B+Shahsavari%2C+M.%3B](http://ieeexplore.ieee.org/iel5/6211/16590/00766087.pdf?tp=&arnu
mber=766087&isnumber=16590&arSt=40&ared=43&arAuthor=Al-
Hammadi%2C+B.%3B+Shahsavari%2C+M.%3B)
 4. E-mail firewall uses S/MIME protocol · SHORT COMMUNICATION
Network Security, Volume 1997, Issue 9, September 1997, Pages 6-7
Atoosa Savarnejad,
[http://www.sciencedirect.com/science?_ob=MImg&_imagekey=B6VJG
-3WNN2SR-1-
1&_cdi=6094&_orig=search&_coverDate=09%2F30%2F1997&_sk=980
029990&view=c&wchp=dGLbVtb-
zSkzk&_acct=C000035118&_version=1&_userid=650615&md5=8c2f6f
1f604d5529b2624f8bcdd3d0bf&ie=f.pdf](http://www.sciencedirect.com/science?_ob=MImg&_imagekey=B6VJG
-3WNN2SR-1-
1&_cdi=6094&_orig=search&_coverDate=09%2F30%2F1997&_sk=980
029990&view=c&wchp=dGLbVtb-
zSkzk&_acct=C000035118&_version=1&_userid=650615&md5=8c2f6f
1f604d5529b2624f8bcdd3d0bf&ie=f.pdf)
 5. [http://www-
10.lotus.com/ldd/today.nsf/0/d2b3eda4956e165a85256b1700175f47
?OpenDocument#Using%20S%2FMIME](http://www-
10.lotus.com/ldd/today.nsf/0/d2b3eda4956e165a85256b1700175f47
?OpenDocument#Using%20S%2FMIME)
 6. Classification methods in the detection of new malicious emails ·
ARTICLE Information Sciences, In Press, Corrected Proof, Available
online 10 July 2004, Dong-Her Shih, Hsiu-Sen Chiang and David Yen,
[http://www.sciencedirect.com/science?_ob=ArticleURL&_aset=B-
WA-A-B-AY-MsSAYVW-UUA-AUEYBYEEWW-AUECEDUDWW-
ZBBWZUCZU-AY-U&_rdoc=3&_fmt=full&_udi=B6VOC-4CPBSS1-
1&_coverDate=07%2F10%2F2004&_cdi=5643&_orig=search&_st=13&
_sort=d&view=c&_acct=C000035118&_version=1&_urlVersion=0&_use
rid=650615&md5=baa003fe9aefaba60602401624412d37](http://www.sciencedirect.com/science?_ob=ArticleURL&_aset=B-
WA-A-B-AY-MsSAYVW-UUA-AUEYBYEEWW-AUECEDUDWW-
ZBBWZUCZU-AY-U&_rdoc=3&_fmt=full&_udi=B6VOC-4CPBSS1-
1&_coverDate=07%2F10%2F2004&_cdi=5643&_orig=search&_st=13&
_sort=d&view=c&_acct=C000035118&_version=1&_urlVersion=0&_use
rid=650615&md5=baa003fe9aefaba60602401624412d37)
 7. <http://en.wikipedia.org/wiki/S/MIME>
 8. Design and implementation of secure e-mail system using elliptic curve
cryptosystem · ARTICLE Future Generation Computer Systems,
Volume 20, Issue 2, 16 February 2004, Pages 315-326 Wongoo Lee
and Jaekwang Lee
[http://www.sciencedirect.com/science?_ob=ArticleURL&_aset=B-
WA-A-A-AE-MsSAYZW-UUW-AUEYBEUAWB-AUECEDUEWB-
ZBBWDUDEB-AE-U&_rdoc=2&_fmt=full&_udi=B6V06-49NXY7J-
2&_coverDate=02%2F16%2F2004&_cdi=5638&_orig=search&_st=13&](http://www.sciencedirect.com/science?_ob=ArticleURL&_aset=B-
WA-A-A-AE-MsSAYZW-UUW-AUEYBEUAWB-AUECEDUEWB-
ZBBWDUDEB-AE-U&_rdoc=2&_fmt=full&_udi=B6V06-49NXY7J-
2&_coverDate=02%2F16%2F2004&_cdi=5638&_orig=search&_st=13&)

- _sort=d&view=c&_acct=C000035118&_version=1&_urlVersion=0&_use
rid=650615&md5=89bce9faa937c19f4d7379808cf9be18
9. <http://csrc.nist.gov/publications/nistpubs/800-49/sp800-49.pdf>
 10. <http://www.sans.org/rr/papers/20/739.pdf>

Srikanth Nannapaneni - snannapa@gmu.edu

1. Cryptography and Network security, William Stallings
2. Secure Messaging Using PGP and S/MIME, Rolf Oppliger
3. Applied Cryptography - Protocols, Algorithms and Source Code in C, Second Edition, by Bruce Schneier
4. Programmer's Guide to Internet Mail, by John Rhoton
5. Cryptography and public key infrastructure on the internet, by Iaus schmeh.
6. Tutorial on S/MIME:
<http://www.marknoble.com/tutorial/smime/smime.aspx>
7. S/MIME Working group: <http://www.imc.org/ietf-smime/index.html>
8. <http://www.faqs.org/rfcs/rfc2633.html>
9. <http://lib.ua.ac.be/ibw/PDF/smimeimp.pdf>
10. <http://www.cswl.com/whiteppr/tech/emailsecurity.html>

Swethana Pagadala - spagadal@gmu.edu

1. Enabling e-mail confidentiality through the use of opportunistic Encryption-a paper by Simson L. Garfinkel simsong@lcs.mit.edu
<http://www.simson.net/> MIT Laboratory for Computer Science, NE43-536, Cambridge, MA 02139 .
2. Encryption and Secure E-mail-An overview by-Dahl A.Gerberick,Technology Risk Services.
3. Defective sign and Encrypt in S/MIME-paper by Don Davis.
4. INFOSYSSEC-The Security Portal for information system security professional -<http://www.infosyssec.net/infosyssec/cry2.html>.
5. Secure E-mail Environment(S.E.E)-Mail Business Requirements version 2.2
6. Protecting your e-mail network-
http://www.hp.com/www.solutions/linux/solutions/sendmail/docs/wp_protect_env.pdf.

7. Comparing PGP and S/MIME-
<http://biphome.spray.se?laszlob/pgp/PGP%20and%20s-mime.doc>.
8. Operational Issues, Standards and Privacy-SEINIT(Security for Pervasive Computing World) -Sathya Rao, Telscom.
9. WSEmail: Secure Internet Messaging Based on Web Services - Kevin Lux, Carl A. Gunter, and Michael J. May University of Pennsylvania April 2004.
10. Secure Electronic Mail-Jyrki Heikkinen ,ICL Personal Systems TeamWARE Division / Enterprise Messaging Development.

Rajesh Ravi - rravi@gmu.edu

1. Beginners Guide to secure email using S/MIME:
<http://www.marknoble.com/tutorial/smime/smime.aspx>
2. Paper : Review about S/MIME:
<http://www.itsecurity.com/papers/articsoft18.htm>
3. Website: Specifications of S/MIME: <http://www.imc.org/smime-pgpmime.html>
4. Guide to use S/MIME:
http://www.mozilla.org/projects/security/pki/psm/smime_guide.html
5. S/MIME Working Group: <http://www.imc.org/ietf-smime/index.html>
6. Book: Secure Messaging with PGP and S/MIME by Rolf Oppliger
7. Beginners Guide to secure email using S/MIME:
<http://www.marknoble.com/tutorial/smime/smime.aspx>
8. S/MIME publications by NIST:
<http://csrc.nist.gov/pki/smime/smpubs.htm>
9. S/MIME implementation guide:
<http://lib.ua.ac.be/ibw/PDF/smimeimp.pdf>
10. Paper: <http://www.cswl.com/whiteppr/tech/emailsecurity.html>

Clate Stansbury - clateiii@hotmail.com

1. Guide to Using S/MIME, Newsgroup: netscape.public.mozilla.crypto,
http://www.mozilla.org/projects/security/pki/psm/smime_guide.htm
2. 5-Minute Security Advisor - How Outlook Security Works,
<http://www.microsoft.com/technet/community/columns/5min/5min-207.msp>
3. S/MIME and OpenPGP, <http://www.imc.org/smime-pgpmime.html>

4. Request for Comments: 2311, S/MIME Version 2 Message Specification, <http://www.ietf.org/rfc/rfc2311.txt>
5. Request for Comments: 2312, S/MIME Version 2 Certificate Handling, <http://www.ietf.org/rfc/rfc2312.txt>
6. S/MIME and PKI, Wei Liu, Ph.D, <http://www.proximo.com/tech/smimepki.html>
7. Implementations:
 - <http://josefsson.org/smime.html> (includes source code link)
 - <http://www.cryptlib.orion.co.nz/S%20Mime.htm> (includes a bad link, but other sites brag about this cryptlib implementation)
 - <http://www.securityfocus.com/tools/447/scoreit>
 - <http://csrc.nist.gov/publications/nistpubs/800-49/sp800-49.pdf>
8. Vulnerabilities:
 - http://www.osvdb.org/displayvuln.php?osvdb_id=4197
 - <http://www.schneier.com/smime.html>
 - <http://www-1.ibm.com/support/docview.wss?rs=463&uid=swg21149731>

Secure WWW servers. Security options in the WWW browsers.

Usman Akhtar - uakhtar@gmu.edu

1. <http://portal.acm.org/citation.cfm>: Internet Environment and Outsourcing
2. <http://portal.acm.org/citation.cfm>: A Method for Transparent Admission Control and Request Scheduling in E-Commerce Web Sites
3. http://www.meer.net/~ericm/papers/ssl_servers.html
4. <http://csdl.computer.org/comp/mags/ic/2002/06/w6038abs.htm>: Developing Secure Web Applications
5. <http://csdl.computer.org/comp/mags/ic/1998/06/w6046abs.htm>: Secure Web Scripting
6. <http://csdl.computer.org/comp/proceedings/icoi/2001/0951/00/09510259abs.htm>: Design and Implementation of Secure Web-based LDAP Management System

7. <http://csdl.computer.org/comp/proceedings/date/2003/1870/01/187011140abs.htm>: Secure Web-Based Framework for Electronic System Level Design
8. <http://csdl.computer.org/comp/proceedings/ride/2004/2095/00/20950056abs.htm>: Exploring a Multi-Faceted Framework for SoC: How to Develop Secure Web-Service Interactions
9. <http://csdl.computer.org/comp/mags/co/2003/10/rx014abs.htm> -: Taking Steps to Secure Web Services
10. <http://csdl.computer.org/comp/proceedings/wet-ice/1997/7967/00/79670269abs.htm>: Secure Workflow Environment

Mayur Enjamoori - menjamoo@gmu.edu

1. <http://trustix.com/web/small/whitepaper.html>
2. http://www.sage-inc.com/cgi-bin/products_bservii.php
3. <http://www.mbedthis.com/products/appWeb/secure-web-servers.html>
4. <http://www.getonline.co.uk/faq/secure-servers/faq-04/>
5. http://www.zeus.com/solutions/security/secure_web_serving.html
6. <http://www-106.ibm.com/developerworks/tivoli/security/>

Zonayed Faruque - zonayed@gmail.com

1. Increase Your Browsing and E-Mail Safety:
<http://www.microsoft.com/security/incident/settings.msp>
2. Browser configuration, tips, hints and security:
<http://www.cexx.org/gofaster.htm>
3. HP OpenVMS systems - Secure Web Browser:
<http://h71000.www7.hp.com/openvms/products/ips/cswb/cswb.html>
4. Building a secure web browser:
<http://www.research.att.com/~smb/papers/sub-browser.pdf>
5. The Secure Sockets Layer Protocol - Enabling Secure Web Transactions: <http://www.itsecurity.com/papers/rainbow3.htm>
6. Security Issues and Solutions, Part 6: Web and TCP/IP Services Security:

- <http://www.awprofessional.com/articles/article.asp?p=26014&seqNum=5>
7. Secure Web Connections :
<http://www.its.ipfw.edu/docs/comm/secure.html>
 8. Secure Shell in a Web Browser:
<http://www2.essex.ac.uk/cs/services/ssh/web.htm>
 9. Browsing for secure alternative browsers :
<http://www.computerworld.com/securitytopics/security/story/0,10801,95326,00.html?SKC=security-95326>
 10. WWW CONSORTIUM:
<http://www.w3.org/Security/Faq/wwwsf2.html>

Jon Halperin- jmhalper@cox.net

1. http://news.zdnet.com/2100-3513_22-5378366.html?tag=zdfd.newsfeed Microsoft will not support IE security functions for any OS but XP.
2. Exploit of windows IE jpg made public
<http://it.slashdot.org/it/04/09/23/1151233.shtml?tid=128>
3. http://news.zdnet.com/2100-9588_22-5368302.html Firefox support grows as people distrust the security in IE.
4. http://news.zdnet.com/2100-1009_22-5378260.html?tag=default IE is susceptible to an attack from jpg pictures.
5. IE flaw may boost browsers http://news.zdnet.com/2100-1009_22-5250697.html
6. Why IE is unsafe to use http://news.zdnet.com/2100-3513_22-5322759.html
7. <http://wp.netscape.com/eng/ssl3/draft302.txt> SSL specifications
8. http://www.usatoday.com/tech/news/computersecurity/2004-09-08-zombieinfect_x.htm USA today- ways to secure your computer, Do not use IE.
9. http://reviews-zdnet.com.com/Mozilla_FireFox_1_OPR/4505-9241_16-31117280-2.html?tag=top Review of FireFox by Cnet.com
10. Securing apache web server with SSL
<http://itpapers.zdnet.com/abstract.aspx?docid=80609&promo=999222&kw+=apache>

Aparna Kasturi - akasturi@gmu.edu

1. Security in computing - Charles P. Fleeger , SL Fleeger, Third Edition.
2. The world wide web: Past Present and Future - Tim Berners Lee Aug 1996
3. www.cybertelecom.org/security
4. An intergrated solution for secur group communication in wide area networks --DA Agarwal, O cherassut,M.R. Thompson, Lawerence Bekerly National lab G Tsudik , University of California, Irvine.
5. Issues on Information access through world wide web- ching - Shan Peng, Jen-Yao Chung, and Kwei-Jay Lin Department og ECE IBM Thomas J watson research centre , University of California, Irvine.
6. Secure workflow environment R.Valia, Y AL Salqan , IEEE compueter society
7. A secure platform for peer to peer computing in the internet. , Wooyoungkim, Sven Graupner and Akhil Sahai-- proceedings of the 35th Hawii International conference on system sciences - 2002
8. Devoloping secure web applications, David Scott, Richard Sharp IEEE transaction Nov/Dec 2002 Vol 6 No 6.
9. Secure and efficient schemes to entrust the use of private keys Kil-ho Shin, IEEE 8th international workshop on enabling technologies: Infrastructure for collaborative Enterprises June 16-18 , 1999
10. Privacy and security in location enhanced world wide web, Jason I Hong, Gaetano Borlrello, James A landay, David W Mc Donald, Bill N Schilit , J.D. Tygar.

Sheryl Pinto - spinto@gmu.edu

1. http://www.secinf.net/websecurity/WWW_Security/Surfing_Between_the_Flags_Security_on_the_Web.html
2. <http://www.virtualschool.edu/mon/ElectronicFrontier/RSA Teseria.html>
3. Book: Applied cryptography and network security : first international conference, ACNS 2003, Kunming, China, October 16-19, 2003 :

proceedings / Jianying Zhou, Moti Yung, Yongfei Han, (eds.) "Trust on Web Browser: Attack vs Defense"

4. Book: WWW security : how to build a secure World Wide Web connection by Robert S. Macgregor, Alberto Aresi, Andreas Siegert

Own topics

Secure Teleconferences over Public Switched Telephone Networks

Inja Youn - iyoun@gmu.edu

1. Youn I, Wijesekera D. Secure Bridges: A Means to Conduct Secure Teleconferences over Public Telephones. Proceedings of IFIP WG 11.3 Working Conference on Data and Application Security pages 205-218, Sitges, Spain, 2004.
2. Katzela I. OPNET. Computer Networks. Computer Simulation. Prentice Hall, 1999.
3. AT&T Webpage,
www.att.com/technology/technologists/fellows/lawser.html
4. J. G. von Bosse. Signaling in Telecommunication Networks. John Wiley & Sons, New York, 1998.
5. CPKtec Research Labs web page,
<http://www.cpktec.com/performance.html>.
6. Specifications of Signaling System No. 7--Message Transfer Part Signaling Performance.
7. ITU-T Recommendation Q.706, March 1993.
8. Specifications of Signaling System No. 7--Signaling performance in the Telephone Application. ITU-T Recommendation Q.706, March 1993. Stage 3 description for multiparty supplementary services using DSS 1. ITU-T. Recommendation, Q.954, 1993.
9. Stage 3 description for multiparty supplementary Specifications of signaling system no. 7. ITU-T Recommendation Q.734, 1993.
10. Stage 2 description for multiparty supplementary services. ITU-T Recommendation Q.84, 1993.
11. Specifications of Signaling System No.7--Hypothetical Signaling Reference Connection. ITU-T Recommendation Q.709, March 1993.
12. G. Lorenz, T. Moore, J. Hale, and S. Sheno. Securing SS7 Telecommunications Networks. In Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, June 2001.
13. T. Russell. Signaling system #7. McGraw-Hill, New York, 2002.
14. R. Sailer. Security in an Open Service Environment. In Proceedings of the Fourteenth Annual Computer Security Applications Conference, pages 223-234, December 1998.

15. M. Sharif, D. Wijesekera. Providing Voice Privacy Over Public Switched Telephone Networks. Proceeding of IFIP, pp 25-36, May 26-28, 2003, Athens, Greece, 2003.
16. Telcordia Technologies Generic Requirements GR-1364-CORE, Issue 1, LSSGR: Switch Processing Time Generic Requirements, Section 5.6, June 1995.
17. Telcordia and ITU-T specification, summarized in IETF Signaling Transport Working Group internet draft (October 22 1999).
18. Department of Defense Security Institute, STU-III Handbook for Industry, <http://www.tscm.com/STUIIIhandbook.html>, February 1997
19. Carne, E. B., Telecommunications Primer, Second Edition, Prentice Hall PTR, Upper Saddle River, New Jersey, 1999.
20. Chlamtac, I., and Lin, Y., Wireless and Mobile Network Architectures, John Wiley & Sons, New York, 2001.
21. ISAAC security research group, GSM Cloning, <http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html>, <http://www.isaac.cs.berkeley.edu/isaac/gsm.html>.
22. Rose, G., Authentication and Security in Mobile Phones, <http://people.qualcomm.com/ggr/QC/AUUG99AuthSec.pdf>
23. Scourias, J., Overview of the Global System for Mobile Communications, <http://ccnga.uwaterloo.ca/~jscouria/GSM/gsmreport.html>.
24. SecureLogix, TeleVPN, <http://www.securelogix.com> , June 2003.

Steganography

Rob Carey - rcarey@gmu.edu

1. Steganography: Why it Matters in a "Post 911" World, <http://www.sans.org/rr/papers/12/676.pdf>
2. Info Stego Personal Edition 3.0, <http://www.antiy.net/infostego/>
3. Whitespace steganography, <http://www.darkside.com.au/snow/>
4. Hide and Seek: An Introduction to Steganography, IEEE Security & Privacy May-June 2003, pg 32-44
5. Steganography by Neil F. Johnson, <http://www.jjtc.com/stegdoc/steg1995.html>

6. Steganography- See No Evil, Hear No Evil, Speak No Evil by Chris Farrow, http://www.giac.org/practical/Chris_Farrow_GSEC.doc
7. Attacks on Steganographic Systems, os.inf.tu-dresden.de/~westfeld/publikationen/ihw99.pdf
8. Steganalysis: The Investigation of Hidden Information, by Neil F. Johnson and Sushil Jajodia. IEEE Information Technology Conference , Syracuse, New York , USA, September 1st - 3rd, 1998: 113-116.
9. Information Hiding Techniques for Steganography and Digital Watermarking, by Stefan Katzenbeisser, Fabien, A.P. Petitcolas
10. Information Hiding : Steganography and Watermarking - Attacks and Countermeasures by Neil F. Johnson, Zoran Duric, Sushil Jajodia

Hardrive Encryption

Rob Carey - rcarey@gmu.edu

1. Encryption by Brett Glass, <http://www.pcmag.com/article2/0,1759,1094425,00.asp>
2. ScramDisk - Disk Encryption Tool, <http://www.securiteam.com/tools/5VP011FOBY.html>
3. Hard Disk Encryption, http://www.infoanarchy.org/wiki/wiki.pl?Hard_Disk_Encryption
4. Inside Encrypting File System by Mark Russinovich, <http://www.winntmag.com/Articles/Index.cfm?ArticleID=5387&Key=Internals>
5. Locking Down Your Data with Cipher Shield External Hard Drive Encryption, <http://www.tomshardware.com/storage/20040916/>
6. Best Possible Privacy Disk Ultra-secure File, Volume and NTFS, www.ciphers.de/downloads/bpp_disk_white_paper_en.pdf
7. LOphT Security Advisory FWB Hard Disk Toolkit, <http://freaky.staticusers.net/fwb.html>
8. Hacking EFS, http://www.sans.org/newsletters/hacking_efs1.htm
9. Hush Encryption Engine White Paper, http://corp.hush.com/info_center/document_library/hush_patent_wp.pdf

10. Entire Hard Disk Encryption vs Virtual Hard Disk Encryption,
http://www.reflex-magnetics.co.uk/files/EHD_Encryption_vs_VHD_Encryption.pdf

SSL Keys on webservers, software and hardware encryption and decryption

Brent McClain - bmcclai1@gmu.edu

1. "SSL Survey", SecuritySpace, Sept. 1st 2004,
http://www.securityspace.com/s_survey/sdata/200408/
2. "OpenSSL v 0.9.7d", OpenSSL Project, 2004, <http://www.openssl.org>
3. "Implementing and using SSL to secure HTTP Traffic", Linux Online, 2004, <http://www.linux.org/docs/ldp/howto/Apache-WebDAV-LDAP-HOWTO/ssl.html>
4. "Apache v2.0.51", Apache HTTP Server Project, 2004,
<http://httpd.apache.org>
5. "SSL Key Password Retrieval Tool", Beyond Security, C. Zacek; F. Russell, 2002, <http://www.securiteam.com/tools/5APOB1F6OG.html>
6. "Performance analysis of elliptic curve cryptography for SSL", International Conference on Mobile Computing and Networking; Proceedings of the ACM workshop on Wireless security, V. Gupta; S. Gupta; S. Chang; D. Stebila, 2002,
<http://portal.acm.org/citation.cfm?id=570691&coll=Portal&dl=GUIDE&CFID=27771150&CFTOKEN=34303943>
7. "Secure Sockets Layer and Transport Layer Security", Communication Networks 2nd Ed, Widjaja, 2004, pg 782-788.
8. "Secure Blue: An Architecture for a Scalable, Reliable, High Volume SSL
9. "Internet Server", 17th Annual Computer Security Applications Conference, R. Mraz, 2001, p 391
10. "The SSL Protocol v3.0", Netscape Inc, A. Freier; P. Karlton; P. Kocher, 1996, <http://wp.netscape.com/eng/ssl3/ssl-toc.html>
11. "The TLS Protocol - Version 1.0", IETF RFC 2246, T. Dierks; C. Allen, 1999, <http://www.ietf.org/rfc/rfc2246.txt>.

VOIP Encryption

Brent McClain - bmcclai1@gmu.edu

1. "VoIP provider to block eavesdroppers", News.Com, B. Charny, March 30, 2004, <http://news.com.com/2100-7352-5181428.html>
2. "FCC Says VoIP Subject to Wiretap Laws", Wi-Fi Planet, R. Mark, August 4, 2004, <http://www.wi-fiplanet.com/voip/article.php/3390671>
3. "VoiceFinder AP2520S Secure VoIP Gateway", AddPac Technology, <http://www.addpac.com/english/AP2520S.html>
4. "Skype: Sliced Bread or Snake Oil?", Strike the Root, J. Blow, Oct 14, 2003, <http://www.strike-the-root.com/3/blow/blow6.html>
5. "VOIP Encryption", Search Networking, Tom Lancaster, 2003, http://www.searchNetworking.com/tip/1,289483,sid7_gci930136,00.html
6. "Fahrenheit FBI", VoIP News, D. McCullagh, August 9th 2004, <http://www.voip-news.com/art/3y.html>
7. "To Whom May I Direct Your Free Call?", New York Times, N. Thompson, Oct. 12, 2003, <http://www.nytimes.com/2003/10/12/business/yourmoney/12kaza.html?position=top&ei=5070&en=5d1c3a0a8566e304&ex=1095912000&adxnnl=1&pagewanted=all&adxnnlx=1095811600-+XoNidkJtKR20uOQX7ChMg>
8. "PGPFone 2.1", PGPI, <http://www.pgpi.org/products/pgpfone/>
9. "Polycom KOs Proprietary VoIP Woes", Network Computing, P. Morrissey, August 21, 2003, <http://www.networkcomputing.com/1416/1416f2.html>
10. "Voice over IPsec: Analysis and Solutions", 18th Annual Computer Security Applications Conference, R. Barbieri; D. Bruschi, E. Rosti, Dec 2002, p 261.

Implementation and analysis of public key Cryptography using RSA Algorithm

Harini Vasudevan - hvasudev@gmu.edu

1. http://www.di-mgt.com.au/rsa_alg.html
2. <http://pajhome.org.uk/index.html>
3. <http://hal.lamar.edu/~KOH/3325/rsa.htm>

4. <http://www.ams.org/bull/2004-41-03/S0273-0979-04-01011-0/S0273-0979-04-01011-0.pdf>
5. http://www.dcs.napier.ac.uk/~bill/wang/r_chap05.pdf
6. Communication Networks, Alberto Leon-Garcia
7. <http://ashvin.flatirons.org/projects/crackingthecode/index.html>
8. http://www.giac.org/practical/GSEC/Carlos_Frederico_Cid_GSEC.pdf
9. <http://home.mweb.co.za/gr/grrr/GrahamRichter/>
10. <http://www.codeproject.com/jscript/JscriptRSA.asp>