Past to Present Cryptographic Systems Used for Commercial and Personal Purposes

Sean Connolly

The Evergreen State College

Methods of Applied Mathematics

professorpi@hotmail.com

May 21, 2005

Abstract

Introduction

DES

Public Key Cryptography

Electronic Signatures

Conclusion

Bibliography

[1] Steven Levy, *Crypto* Viking Penguin, New York, 1984.

[2] Alfred J. Menezes, Paul C van Oorshot, and Scott A. Vanstone, *Handbook of Applied Cryptography* CRC Press, New York, 1997.

[3] Cary Meltzer and Doris Baker, *Cryptography Decrypted* Addison-Wesley, New York, Second Printing 2001.

[4] Gustavus J. Simmons, *Contemporary Cryptology, The Science of Information Integrity* IEEE Press, New York, 1992.

[5] The Institute for Math and Science Education of the University of Illinois at Chicago, *Cryptography, The Mathematics of Secret Codes* http://cryptoclub.math.uic.edu/about/aboutbook.htm, 2004.

[6] Greg Sterijevski, *The Data E,cryption Standard* http://raphael.math.uic.edu/ jeremy/crypt/contrib/stj.html, Retrieved 2005.

[7] Arnoud Engelfriet, *The DES encryption algorithm* http://www.iusmentis.com/technology/encryption/des/, 2003.

[8] Arnoud Engelfriet, *The DES enc,yption algorithm* http://www.itl.nist.gov/fipspubs/fip46-2.htm, 2003.

[9] some guy, *public* don't know yet, 2003.

[10] Dave Rudolf, *Optimized Differential Cryptanalysis of the Data Encryption Standard* University of Saskatchewan, http://davrud.sasktelwebsite.net/programming/des/, 2001.