1. Record Nr. UNINA9910830574403321

Autore	Stamp Mark
Titolo	Applied cryptanalysis : breaking ciphers in the real world / / Mark Stamp, Richard M. Low
Pubbl/distr/stampa	Hoboken, New Jersey : , : Wiley-Interscience, , c2007
ISBN	1-280-90120-9 9786610901203 0-470-14877-2 0-470-14876-4
Descrizione fisica	1 online resource (424 p.)
Altri autori (Persone)	LowRichard M. <1967->
Disciplina	005.82
Soggetti	Computer security Data encryption (Computer science) Cryptography
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	"A John Wiley & Sons, Inc., publication."
Nota di bibliografia	Includes bibliographical references (p. 375-392) and index.
Nota di contenuto	Preface -- About The Authors -- Acknowledgments -- 1. Classic Ciphers -- 1.1 Introduction -- 1.2 Good Guys and Bad Guys -- 1.3 Terminology -- 1.4 Selected Classic Crypto Topics -- 1.4.1 Transposition Ciphers -- 1.4.2 Substitution Ciphers -- 1.4.3 One-Time Pad -- 1.4.4 Codebook Ciphers -- 1.5 Summary -- 1.6 Problems -- 2. World War II Ciphers -- 2.1 Introduction -- 2.2 Enigma -- 2.2.1 Enigma Cipher Machine -- 2.2.2 Enigma Keyspace -- 2.2.3 Rotors -- 2.2.4 Enigma Attack -- 2.2.5 More Secure Enigma -- 2.3 Purple -- 2.3.1 Purple Cipher Machine -- 2.3.2 Purple Keyspace -- 2.3.3 Purple Diagnosis -- 2.3.4 Decrypting Purple -- 2.3.5 Purple versus Enigma -- 2.4 Sigaba -- 2.4.1 Sigaba Cipher Machine -- 2.4.2 Sigaba Keyspace -- 2.4.3 Sigaba Attack -- 2.4.4 Sigaba Conclusion -- 2.5 Summary -- 2.6 Problems -- 3. Stream Ciphers -- 3.1 Introduction -- 3.2 Shift Registers -- 3.2.1 Berlekamp-Massey Algorithm -- 3.2.2 Cryptographically Strong Sequences -- 3.2.3 Shift Register-Based Stream Ciphers -- 3.2.4 Correlation Attack -- 3.3 ORYX -- 3.3.1 ORYX Cipher -- 3.3.2 ORYX Attack -- 3.3.3 Secure ORYX -- 3.4 RC4 -- 3.4.1 RC4 Algorithm -- 3.4.2 RC4 Attack -- 3.4.3 Preventing the RC4 Attack

-- 3.5 PKZIP -- 3.5.1 PKZIP Cipher -- 3.5.2 PKZIP Attack -- 3.5.3 Improved PKZIP -- 3.6 Summary -- 3.7 Problems -- 4. Block Ciphers -- 4.1 Introduction -- 4.2 Block Cipher Modes -- 4.3 Feistel Cipher -- 4.4 Hellman's Time-Memory Trade-Off -- 4.4.1 Cryptanalytic TMTO -- 4.4.2 Bad Chains -- 4.4.3 Success Probability -- 4.4.4 Distributed TMTO -- 4.4.5 TMTO Conclusions -- 4.5 CMEA -- 4.5.1 CMEA Cipher -- 4.5.2 SCMEA Cipher -- 4.5.3 SCMEA <st1:place w:st="on" >Chosen</st1:place> Plaintext Attack -- 4.5.4 CMEA <st1:place w: st="on">Chosen</st1:place> Plaintext Attack -- 4.5.5 SCMEA Known Plaintext Attack -- 4.5.6 CMEA Known Plaintext Attack -- 4.5.7 More Secure CMEA -- 4.6 Akelarre -- 4.6.1 Akelarre Cipher.
4.6.2 Akelarre Attack -- 4.6.3 Improved Akelarre? -- 4.7 FEAL -- 4.7.1 FEAL-4 Cipher -- 4.7.2 FEAL-4 Differential Attack -- 4.7.3 FEAL-4 Linear Attack -- 4.7.4 Confusion and Diffusion -- 4.8 Summary -- 4.9 Problems -- 5. Hash Functions -- 5.1 Introduction -- 5.2 Birthdays and Hashing -- 5.2.1 The Birthday Problem -- 5.2.2 Birthday Attacks on Hash Functions -- 5.2.3 Digital Signature Birthday Attack -- 5.2.4 Nostradamus Attack -- 5.3 MD4 -- 5.3.1 MD4 Algorithm -- 5.3.2 MD4 Attack -- 5.3.3 A Meaningful Collision -- 5.4 MD5 -- 5.4.1 MD5 Algorithm -- 5.4.2 A Precise Differential -- 5.4.3 Outline of Wang?s Attack -- 5.4.4 Wang's MD5 Differentials -- 5.4.5 Reverse Engineering Wang's Attack -- 5.4.6 Stevens' Attack -- 5.4.7 A Practical Attack -- 5.5 Summary -- 5.6 Problems -- 6. Public Key Systems -- 6.1 Introduction -- 6.2 Merkle-Hellman Knapsack -- 6.2.1 Lattice-Reduction Attack -- 6.2.2 Knapsack Conclusion -- 6.3 Diffie-Hellman Key Exchange -- 6.3.1 Man-in-the-Middle Attack -- 6.3.2 Diffie-Hellman Conclusion -- 6.4 Arithmetica Key Exchange -- 6.4.1 Hughes-Tannenbaum Length Attack -- 6.4.2 Arithmetica Conclusion -- 6.5 RSA -- 6.5.1 Mathematical Issues -- 6.5.2 RSA Conclusion -- 6.6 Rabin Cipher -- 6.6.1 Chosen Ciphertext Attack -- 6.6.2 Rabin Cryptosystem Conclusion -- 6.7 NTRU Cipher -- 6.7.1 Meet-in-the-Middle Attack -- 6.7.2 Multiple Transmission Attack -- 6.7.3 Chosen Ciphertext Attack -- 6.7.4 NTRU Conclusion -- 6.8 ElGamal Signature Scheme -- 6.8.1 Mathematical Issues -- 6.8.2 ElGamal Signature Conclusion -- 6.9 Summary -- 6.10 Problems -- 7. Public Key Attacks -- 7.1 Introduction -- 7.2 Factoring Algorithms -- 7.2.1 Trial Division -- 7.2.2 <st1:City w:st="on"><st1:place w:st="on">Dixon</st1:place></st1:City>'s Algorithm -- 7.2.3 Quadratic Sieve -- 7.2.4 Factoring Conclusions -- 7.3 Discrete Log Algorithms -- 7.3.1 Trial Multiplication -- 7.3.2 Baby-Step Giant-Step -- 7.3.3 Index Calculus.
7.3.4 Discrete Log Conclusions -- 7.4 RSA Implementation Attacks -- 7.4.1 Timing Attacks -- 7.4.2 Glitching Attack -- 7.4.3 Implementation Attacks Conclusions -- 7.5 Summary -- 7.6 Problems -- Appendix -- A-1 MD5 Tables -- A-2 Math -- A-2.1 Number Theory -- A-2.2 Group Theory -- A-2.3 Ring Theory -- A-2.4 Linear Algebra -- Annotated Bibliography -- Index.

Sommario/riassunto

The book is designed to be accessible to motivated IT professionals who want to learn more about the specific attacks covered. In particular, every effort has been made to keep the chapters independent, so if someone is interested in has function cryptanalysis or RSA timing attacks, they do not necessarily need to study all of the previous material in the text. This would be particularly valuable to working professionals who might want to use the book as a way to quickly gain some depth on one specific topic.