

To help you order the material in our past 4 lectures, I have put together a Index to Lectures, Table of Figures and Table of Tables for Lectures 19-22.

CLASSICAL CRYPTOGRAPHY COURSE

Index to Lectures 19-22

BY
LANAKI

17 January 1997

CONTENTS

LECTURE 19: PASSWORDS, PRIVACY, DATA PROTECTION

Summary
Password Vulnerability
UNIX Vulnerability
Collection
Klein's Survey
Safe Passwords?
Methods of Attack
1. Name Variations
2. Dictionaries
3. Permutations of Item 2
4. Capitalization
5. Foreign Words
6. Word Pairs
Summary of results
Privacy References/ Resources
Introduction to Privacy Issues
MIB
NCOA
NCIC
Privacy and other Personal Rights
The Federal Privacy Act 1988
State Acts and Regulations
Employee Rights
International Privacy
A Deeper Look at Electronic Mail
Data Protection and Data Encryption: A View Of Modern Challenges
Trusted Information Systems
Classical Cryptography / Recreational Cryptography
The U.S. International Trade in Arms Regulations (ITAR)
ITAR Exceptions
Purpose Of Encryption
Modern Cryptography: Using Private and Public Cryptographic Keys
Data Encryption Standard (DES)
Key Distribution Drawback
Rivest, Shamir, and Adleman Algorithm (RSA)
Cryptographic Networks
Pretty Good privacy (PGP)
Privacy Enhanced Mail (PEM)
Key Management and Distribution
Implementation Considerations
Media
Configurations
One-Time Cipher Keys
Digital Signatures and Notations
Carte A Memoir (Memory Card)

Cyber Notaries
KERBEROS
TEMPEST
The CLIPPER/SKIPJACK Chip Controversy
Lecture 18 Solutions
Appendix 1: TIS Worldwide Survey of Cryptographic
Manufacturers and Developers of Cryptographic Products -

Crypto Survey -Domestic Products: Summary listing of domestic cryptographic products as of 7/25/96

Crypto Survey - Foreign Products Summary listing of foreign cryptographic products as of 7/25/96

Appendix 2 : Bernstein vs United States Crypto Case
Case Background
Legal Arguments
Full text Available

Appendix 3 : Federal Register, Vol. 58, No. 139 Rules and Regulations Department Of State Bureau
of Politico-Military Affairs 22 CFR Parts 120, 121, 122, 123, 124, 125, 126, 127, 128,
and 130 [Public Notice 1832] Amendments to the International Traffic in Arms
Regulations Part II 58 FR 39280 Date: Thursday, July 22, 1993 Action: Final rule.

PART 121 - The United States Munitions List Category XIII-Auxiliary Military Equipment

Appendix 4: Clinton's Encryption Plan with Key recovery System

LECTURE 20: CODES

Summary
Code Systems
Trithem Code Book
>From Lloyd to Marconi
ABC Code
Morse Code
U. S. COAST GUARD Discontinues Morse Code
Commercial Codes
Marconi Code
Non-Secret Codes
ACME Seven Digit Codebook
Encoding
Decoding
Brevity Codes
International Code Of Signals For Visual, Sound and
Radio Communications (INTERCO)
Basics of Code Construction
Parallel Sets
Two- Letter Differential
Types
Enciphered Code System
Dictionary Codes
Cryptanalysis Of a Simple Dictionary Code
Diplomatic Codes

LECTURE 21: CRYPTANALYSIS OF THE NAVY CSP 1500 CIPHER MACHINE [HAGELIN C-38 FAMILY]

Summary

Machine Cipher Systems
Transposition Cipher Machines
Substitution Cipher Machines
Hagelin C-38 Cipher Machine Family
Pics
Wheels or Rotors
The Squirrel-Cage
Letter Encipherment
An Example Of Key Generation In the CSP 1500
Message Encipherment
Cryptanalysis Of the CSP 1500
Word Spacing with the Letter Z
Analysis of a Single - Wheel CSP 1500 Cipher Machine
Analysis of a Two - Wheel CSP 1500 Cipher Machine
Analysis of a Three - Wheel CSP 1500 Cipher Machine
Analysis of a Four - Wheel CSP 1500 Cipher Machine
Monoalphabets
Lugs
Analysis of a Six - Wheel CSP 1500 Cipher Machine
Special Case 1 - Indicators are Unenciphered.
Stripping off the Generated Key
Pin and Lug Settings
Enciphered Indicators
Special Case 2 - Operator Error and Stagger
General Solution of Six - Wheel CSP 1500 Cipher Machine

LECTURE 22 : CIPHER MACHINES II HEBERN'S "COMMERCIAL PORTABLE CODE" MACHINE AND THE ELECTRONIC CIPHER MACHINE MARK II (ECM MARK II or SIGABA)

Summary

Acknowledgments
Introduction to Machine Cryptography
Hebern Commercial Portable Code Machine
Step 1: Rewrite the Ciphertext
Step 2: Make a Frequency Tableau
Step 3: Match the diagonal alphabets
Step 4: Construct the Reduction Tableau
Step 5: Monoalphabetic Ciphertext
History of the ECM MARK II
Two Views Of the ECM MARK II'S Development
Navy Systems
Army Systems
Combined US - British System - CSP 1700
Destruction of a National Treasure
USS PAMPANITO (SS-383)
Cipher Equipment Aboard PAMPANITO During 1944:
Details Of ECM MARK II Cipher Unit
SIGABA Grouping Of Output From Control Rotors To Index Rotors
Appendix 1 : USS PAMPANITO (SS-383) The Third War Patrol
August 17 - September 28, 1944
Appendix 2 : Replica Operating Instructions for ASAM 1
(a.k.a. ECM Mark II)
Appendix 3 : Keying (Operating) The ECM MARK II
Appendix 4 : Compliance with Operating Procedures
Appendix 5 : ECM Mark II Specifications
Additional References

TABLES

Table 19-1: Passwords Cracked for Sample Set of 13,797 Accounts
Table 19-2: Length of the cracked passwords.
Table 20-1: Tritheim's Code Alphabets
Table 20-2: Example of ABC Code Page
Table 20-3: Comparative Table of Order Of Morse's Count with Telegraph Frequencies
Table 20-4: Learning Morse Code (Invented by Morse and Symbolization by Morse)
Table 20-5: The First part of the Marconi Code. General Phrases Code words, Five letters
Table 20-6a: page 3, 3rd, 4th, and 5th Figures Third and Fourth Letters
Table 20-6b: page 6, 3rd, 4th, and 5th Figures Third and Fourth Letters
Table 20-7: Sample Entries from INTERCO Codebook
Table 20-8: Phonetic Alphabet used with INTERCO
Table 20-9: One-part Code
Table 20-10: Two-part code
Table 20-11: Caption Code
Table 20-13: Indicators and Key Blocks
Table 20-14: Digraphic Equivalentents for Superencipherment
Table 20-15: 1/3 Sample page WE029
Table 20-16: Countries in which WE029 was used and Service
Table 21-1: C-38 Hagelin Cipher Machine (CSP1500) Beaufort Tableau
Table 21-2: Operational Wheel Settings CSP1500

FIGURES

Figure 19-1: Fully Connected End-To-End Network
Figure 19-2: Link Encrypted Network
Figure 19-3: Hybrid Network
Figure 19-4: Central Key Distribution Facility
Figure 22-1: Column Frequency Counts - Hebern Machine
Figure 22-2: Diagonal Column Frequency Count - Hebern Machine
Figure 22-3: Reduction Tableau
Figure 22-4: Displacement Values