CS 5602 Lec 01
Introduction to Cryptography (Cryptology)

George Markowsky
Computer Science Department
Missouri University of Science and Technology

1

Course Description

- *COMP SCI 5602 Introduction to Cryptography* (LEC 3.0)
- Introduces fundamentals of modern cryptography. Topics include basic number theory, public & private key encryption schemes, cryptographic hash functions, message authentication codes, elliptic curve cryptography, Diffie-Hellman key agreements, digital signatures, PUFs, quantum cryptography, and generation of prime numbers and pseudo-random sequences. Prerequisites: A grade of "C" or better in COMP SCI 5200 or a grade of "B" or better in COMP SCI 2500.

2

Syllabus

- I hope to have this ready by next Thursday
- Basically, you will have homeworks, 2 Prelims, and 1 Final
- Details on Thursday

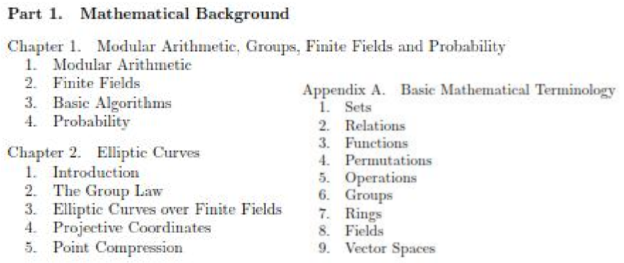
3

Textbooks

- I have posted two free PDF textbooks on Canvas
- The primary text will be Nigel Smart's Cryptography: An Introduction (3rd Edition)
- The secondary text will be Al Sweigart's Hacking Secret Ciphers with Python, which is the free, earlier version of Cracking Codes with Python, which is not free
- In addition, there will be additional materials that I will distribute to cover topics not covered in the aforementioned texts

4

Topics (Initial List)



Part 1. Mathematical Background

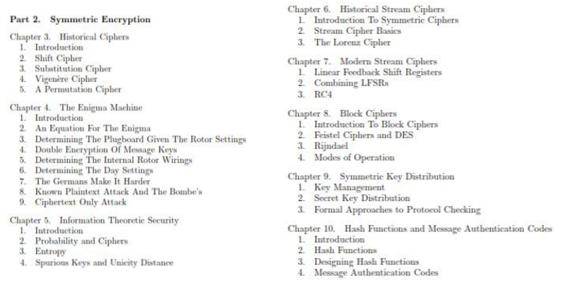
Chapter 1. Modular Arithmetic, Groups, Finite Fields and Probability
1. Modular Arithmetic
2. Finite Fields
3. Basic Algorithms
4. Probability

Chapter 2. Elliptic Curves
1. Introduction
2. The Group Law
3. Elliptic Curves over Finite Fields
4. Projective Coordinates
5. Point Compression

Appendix A. Basic Mathematical Terminology
1. Sets
2. Relations
3. Functions
4. Permutations
5. Operations
6. Groups
7. Rings
8. Fields
9. Vector Spaces

5

Topics (Initial List)



Part 2. Symmetric Encryption

Chapter 3. Historical Ciphers
1. Introduction
2. Shift Cipher
3. Substitution Cipher
4. Vigenère Cipher
5. A Permutation Cipher

Chapter 4. The Enigma Machine
1. Introduction
2. An Equation For The Enigma
3. Determining The Plugboard Given The Rotor Settings
4. Double Encryption Of Message Keys
5. Determining The Internal Rotor Wirings
6. Determining The Day Settings
7. The Germans Make It Harder
8. Known Plaintext Attack And The Bombe's
9. Ciphertext Only Attack

Chapter 5. Information Theoretic Security
1. Introduction
2. Probability and Ciphers
3. Entropy
4. Spurious Keys and Unicity Distance

Chapter 6. Historical Stream Ciphers
1. Introduction To Symmetric Ciphers
2. Stream Cipher Basics
3. The Lorenz Cipher

Chapter 7. Modern Stream Ciphers
1. Linear Feedback Shift Registers
2. Combining LFSRs
3. RC4

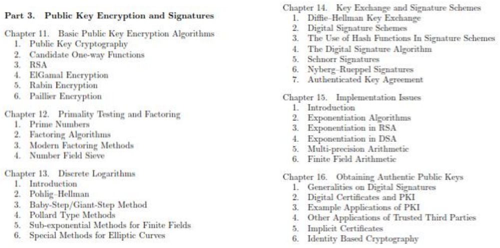
Chapter 8. Block Ciphers
1. Introduction To Block Ciphers
2. Feistel Ciphers and DES
3. Rijndael
4. Modes of Operation

Chapter 9. Symmetric Key Distribution
1. Key Management
2. Secret Key Distribution
3. Formal Approaches to Protocol Checking

Chapter 10. Hash Functions and Message Authentication Codes
1. Introduction
2. Hash Functions
3. Designing Hash Functions
4. Message Authentication Codes

6

Topics (Initial List)



Part 3. Public Key Encryption and Signatures

Chapter 11. Basic Public Key Encryption Algorithms
1. Public Key Cryptography
2. Candidate One-way Functions
3. RSA
4. ElGamal Encryption
5. Rabin Encryption
6. Paillier Encryption

Chapter 12. Primality Testing and Factoring
1. Prime Numbers
2. Factoring Algorithms
3. Modern Factoring Methods
4. Number Field Sieve

Chapter 13. Discrete Logarithms
1. Introduction
2. Pohlig–Hellman
3. Baby-Step/Giant-Step Method
4. Pollard Type Methods
5. Sub-exponential Methods for Finite Fields
6. Special Methods for Elliptic Curves

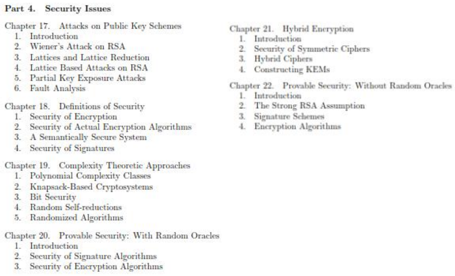
Chapter 14. Key Exchange and Signature Schemes
1. Diffie–Hellman Key Exchange
2. Digital Signature Schemes
3. The Use of Hash Functions In Signature Schemes
4. The Digital Signature Algorithm
5. Schnorr Signatures
6. Nyberg–Rueppel Signatures
7. Authenticated Key Agreement

Chapter 15. Implementation Issues
1. Introduction
2. Exponentiation Algorithms
3. Exponentiation in RSA
4. Exponentiation in DSA
5. Multi-precision Arithmetic
6. Finite Field Arithmetic

Chapter 16. Obtaining Authentic Public Keys
1. Generalities on Digital Signatures
2. Digital Certificates and PKI
3. Example Applications of PKI
4. Other Applications of Trusted Third Parties
5. Implicit Certificates
6. Identity Based Cryptography

7

Topics (Initial List)



Part 4. Security Issues

Chapter 17. Attacks on Public Key Schemes
1. Introduction
2. Wiener's Attack on RSA
3. Lattices and Lattice Reduction
4. Lattice Based Attacks on RSA
5. Partial Key Exposure Attacks
6. Fault Analysis

Chapter 18. Definitions of Security
1. Security of Encryption
2. Security of Actual Encryption Algorithms
3. A Semantically Secure System
4. Security of Signatures

Chapter 19. Complexity Theoretic Approaches
1. Polynomial Complexity Classes
2. Knapsack-Based Cryptosystems
3. Bit Security
4. Random Self-reductions
5. Randomized Algorithms

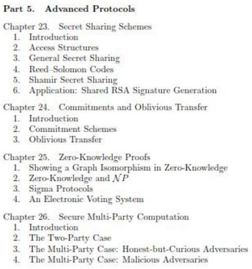
Chapter 20. Provable Security: With Random Oracles
1. Introduction
2. Security of Signature Algorithms
3. Security of Encryption Algorithms

Chapter 21. Hybrid Encryption
1. Introduction
2. Security of Symmetric Ciphers
3. Hybrid Ciphers
4. Constructing KEMs

Chapter 22. Provable Security: Without Random Oracles
1. Introduction
2. The Strong RSA Assumption
3. Signature Schemes
4. Encryption Algorithms

8

Topics (Initial List)



Part 5. Advanced Protocols

Chapter 23. Secret Sharing Schemes
1. Introduction
2. Access Structures
3. General Secret Sharing
4. Reed–Solomon Codes
5. Shamir Secret Sharing
6. Application: Shared RSA Signature Generation

Chapter 24. Commitments and Oblivious Transfer
1. Introduction
2. Commitment Schemes
3. Oblivious Transfer

Chapter 25. Zero-Knowledge Proofs
1. Showing a Graph Isomorphism in Zero-Knowledge
2. Zero-Knowledge and $\mathcal{NP}$
3. Sigma Protocols
4. An Electronic Voting System

Chapter 26. Secure Multi-Party Computation
1. Introduction
2. The Two-Party Case
3. The Multi-Party Case: Honest-but-Curious Adversaries
4. The Multi-Party Case: Malicious Adversaries

9

Today's Lecture

- Some Definitions
- The Importance of Cryptology
- Classical Cryptology
- Modern Cryptology
- Applications of Modern Cryptology
- Brief Survey of Quantum Mechanics
- Quantum Cryptology
- Implications for Computer Science

10

Some Definitions

- Cryptography - the art of providing secure communication over insecure channels.
  - Encode text and provide a method for decoding.
  - No attempt is made to hide the message.
- Cryptanalysis - the art of breaking into cryptographic communication and understanding their contents.

11

Some Definitions

- Cryptology - the combination of Cryptography and Cryptanalysis.
- Cleartext or Plaintext - the original material that is to be transmitted by cryptography.
- Enciphered text - the result when plaintext is encoded.

12

Some Definitions

- Steganography - the art of concealing messages.
  - Shaved heads
  - "Invisible" inks
  - Microdots
  - Pin pricks above letters in books, etc.
  - Of interest to hackers in exporting stolen data

13

Importance of Cryptology

- Military applications: command and control
- Diplomatic applications: information gathering, instructions, spying
- Economic applications
  - Information protection
  - Banking transactions
  - Authentication and signatures

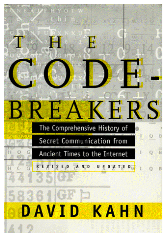
14

Importance of Cryptology

- Privacy
- Amusement and intellectual stimulation
- Foundations of computer science
  - "First" computers built for cryptanalysis in World War II
  - Many key figures of computer science worked in cryptology: Shannon and Turing
- Quantum Cryptography has implications for computer science

15

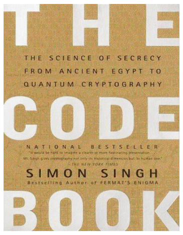
Some References


THE
CODE-
BREAKERS
The Comprehensive History of
Secret Communication from
Ancient Times to the Internet
REVISED AND UPDATED
DAVID KAHN

- Long time standard
- Mostly historical and little technical detail
- Somewhat weak in contemporary developments
- Editions in 1967 and 1996

16

Some References



- Revised paperback version August 2000
- Very highly recommended
- Entertaining and somewhat technical
- Good website with lots of code and examples:
- http://simonsingh.net/books/the-code-book/

17

An Interesting Opportunity

- *Tens of thousands of copies of this resource were downloaded before its 16-bit software became outdated.*
- *The software can still be downloaded for free, but be warned that it is not going to be easy to run it, and we cannot offer any support. Sorry.*
- *I am hoping that one day the software can be updated and re-written so that this terrific crypto resource can be widely used again.*
- *In fact, if you know someone who wants to update the resource for Windows 10 or Mac (perhaps a project for a degree student or masters student), then please get in touch via the contact button.*
- *Or maybe you belong to a company that would like to update the resource – I would certainly consider putting a company logo on every page of the resource.*

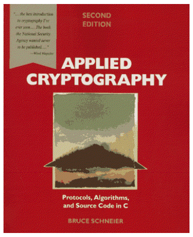
18

Software Details

1. Encryption tools,
2. Code breaking tools,
3. Coded messages to crack,
4. Material for teachers, e.g., worksheets,
5. A realistic, virtual Enigma cipher machine,
6. A beginner's cryptography tutorial,
7. A history of codes from 1000BC to 2000AD,
8. Material for junior codebreakers,
9. An animated section on quantum cryptography,
10. Sections on public key crypto & RSA.

19

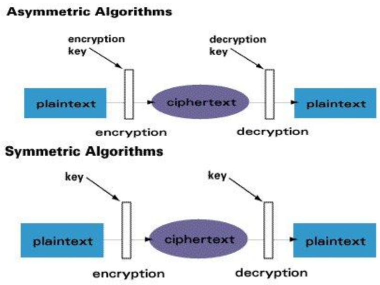
Some References



- This book by Bruce Schneier is a good technical introduction to cryptography
- Cryptography is a fast moving field, so going to conferences is the way to keep current
- New edition in 2015 seems like repackaging of old edition

20

Types of Algorithms



Asymmetric Algorithms

encryption key

decryption key

plaintext

ciphertext

plaintext

encryption

decryption

Symmetric Algorithms

key

key

plaintext

ciphertext

plaintext

encryption

decryption

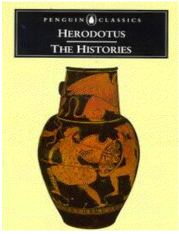
21

Cryptography in Ancient Egypt

- According to Kahn, Egyptians used secret writing as an embellishment to funeral inscriptions
- Allegedly, this enhanced the magic of the deceased

22

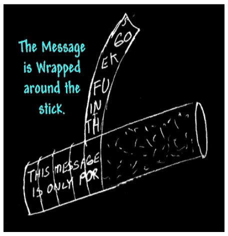
The Greeks and Steganography



- Herodutus states that a warning of the Persian invasion of Greece came from a Greek exile who wrote on wood and covered it with wax.
- Gorgo, a Spartan woman figured out the secret and gave a warning

23

The Greeks and Cryptography



- This is called a *skytale*
- Can be read only around a stick of the correct diameter
- Used in the 5th century BCE by the Spartans
- Instance of a *transposition cipher*

24

Modern Steganography – What do you see?

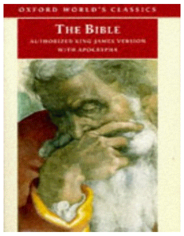
25

Transposition Ciphers

- The idea here is to permute the actual letters of the message in some way
- Some examples are:
  - Reverse pairs of letters
    - HELLO WORLD
    - EHLL OOWLRD
  - Remove every second letter and put it at the end.
    - HELLO WORLD
    - HLOWRDEL OL
  - Reverse the letters
    - HELLO WORLD
    - DLROW OLLEH
- Many trickier transpositions are possible

26

Cryptography in the Bible



- Jewish writers in the Bible used *atbash*, which is a substitution cypher in which the first letter is replaced the last, the second by the next to last, etc.
- Thus, Babylon comes out Sheshach or Sheshech

27

Atbash

- This illustrates how the atbash algorithm works

ABCDEFGHIJKLMNOPQRSTUVWXYZ
ZYXWVUTSRQPONMLKJIHGFEDCBA

XIBKGLTIZKSB

Atbash

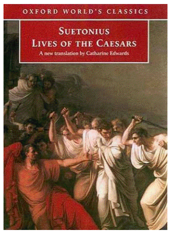
28

Substitution Cyphers

- Atbash is an example of a substitution cypher
- Widely used in various detective stories
  - *The Gold Bug* by Edgar Allan Poe about his detective Legrand
  - *The Adventure of the Dancing Men* by Arthur Conan Doyle about his detective Sherlock Holmes

29

Julius Caeser and Cryptography



- According to Suetonius, Julius Caeser used some simple substitution ciphers
- Below is a substitution cipher where each letter is replaced by a letter 2 further in the alphabet

ABCDEFGHIJKLMNOPQRSTUVWXYZ
YZABCDEFGHIJKLMNOPQRSTUVWX

30

Julius Caeser's Ciphers

- This illustrates how a Caeser cipher works

JULIUS

10

Encrypt

Shift Size

31

Classical Cryptology

- Invented in the Middle East
  - Interested in riddles and puzzles
  - Described advanced variations of substitutions ciphers
  - Introduced frequency analysis of letters and letter combinations
  - Influenced Europeans

32

Substitution Ciphers

- You have some permutation of letters that permits you to substitute one letter for another. *Often will remove blanks.*

ABCDEFGHIJKLMNOPQRSTUVWXYZ

BADCFEHGJILKNMPORQTSVUXWZY

HELLO WORLD → GFKKPXPQKC

33

Analyzing Substitution Ciphers

- Frequency Table
- Can use multiple alphabets, etc.

13	9	8	8	7	7	7	6	6	4	4	3	3	3	3	2	2	2	1	1	1	-	-	-	-	-
E	T	A	O	N	I	R	S	H	L	D	C	U	P	F	M	W	Y	B	G	V	K	Q	X	J	Z

34

Classical Cryptology

- Renaissance political intrigues sparked a resurgence of cryptology
- Leon Battista Alberti (ca. 1465) the Father of Western Cryptology
- Giovanni Soro of Venice the first great Western cryptanalyst
- Cryptanalysis by Thomas Phelippes supplied evidence against Mary, Queen of Scots (ca. 1586)
  - *A weak cipher is worse than no cipher at all*
- Many famous names
- Many countries had *Black Chambers*

35

Modern Communications

- Telegraphy greatly increased volume of cryptographic messages
  - Interception sporadic and difficult
  - Cables can be taped sometimes
- Radio communication made cryptanalysis come into its own
  - Assumption is that enemy has all the text
- Volume of traffic might limit complexity of cryptographic system
  - High speed computers change this

36

Some Early Radio Interception Facilities

Army cryptologists first went to the field during World War I. This site is a mock-up of the World War I Verdun intercept site in France, built by NSA craftsmen based on the two extant pictures of the original shack.

During the early 1900s, the Army operated from mobile as well as fixed installations. The museum displays a picture of a mobile U.S. direction finding truck, or "tractor" in the terminology of the time. The truck had a DF antenna, which was turned by hand from the inside. By measuring the angle of entry and the skip of a signal coming in and bouncing off the ionosphere, an operator could pinpoint the distance the radio wave had travelled - rather advanced for 1918.

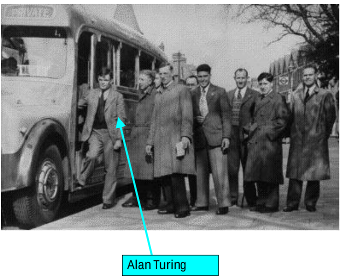
37

Rewriting History

- For a long time, success in cracking enemy codes was covered up even after the relevant wars
- After WW II, many developing nations used German Enigma machines to encode messages
- The British benefited greatly by being able to read many dispatches
- The Battle of Midway won by codebreakers

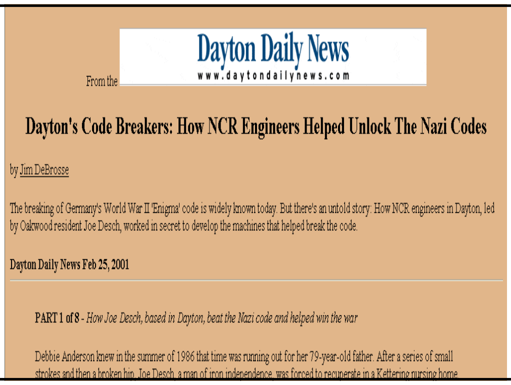
38

Enigma



Alan Turing

39



From the **Dayton Daily News**
www.daytondailynews.com

Dayton's Code Breakers: How NCR Engineers Helped Unlock The Nazi Codes

by Jim DeBrosse

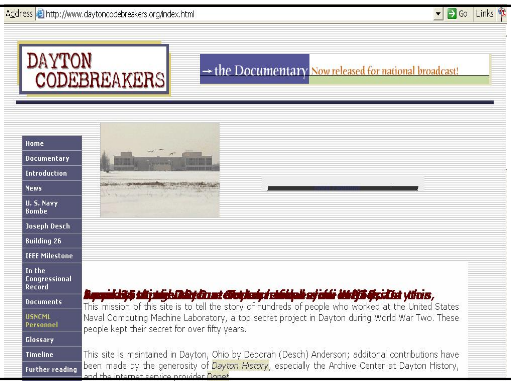
The breaking of Germany's World War II 'Enigma' code is widely known today. But there's an untold story: How NCR engineers in Dayton, led by Oakwood resident Joe Desch, worked in secret to develop the machines that helped break the code.

Dayton Daily News Feb 25, 2001

PART 1 of 8 - *How Joe Desch, based in Dayton, beat the Nazi code and helped win the war*

Debbie Anderson knew in the summer of 1986 that time was running out for her 79-year-old father. After a series of small strokes and then a broken hip, Joe Desch, a man of iron independence, was forced to recuperate in a Kettering nursing home

40



Address http://www.daytoncodebreakers.org/index.html Go Links

DAYTON CODEBREAKERS

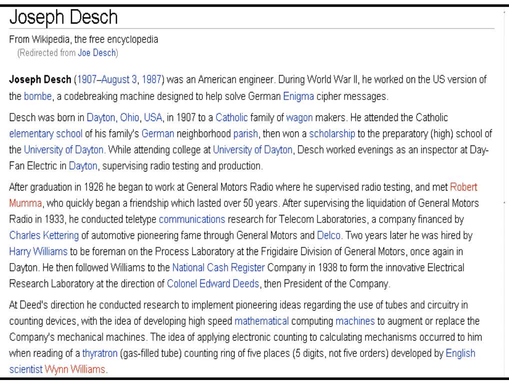
→ the Documentary Now released for national broadcast!

[illegible]

This mission of this site is to tell the story of hundreds of people who worked at the United States Naval Computing Machine Laboratory, a top secret project in Dayton during World War Two. These people kept their secret for over fifty years.

This site is maintained in Dayton, Ohio by Deborah (Desch) Anderson; additonal contributions have been made by the generosity of *Dayton History*, especially the Archive Center at Dayton History, and the internet service provider Donet.

41



Joseph Desch

From Wikipedia, the free encyclopedia
(Redirected from Joe Desch)

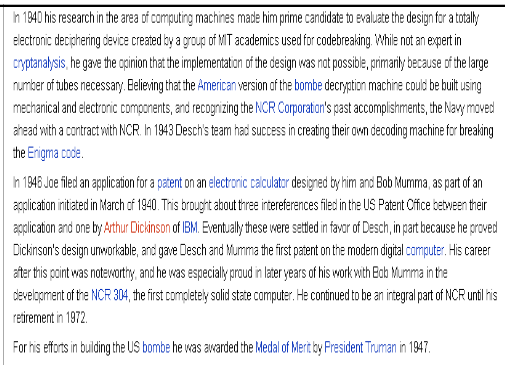
Joseph Desch (1907–August 3, 1987) was an American engineer. During World War II, he worked on the US version of the bombe, a codebreaking machine designed to help solve German Enigma cipher messages.

Desch was born in Dayton, Ohio, USA, in 1907 to a Catholic family of wagon makers. He attended the Catholic elementary school of his family's German neighborhood parish, then won a scholarship to the preparatory (high) school of the University of Dayton. While attending college at University of Dayton, Desch worked evenings as an inspector at Day-Fan Electric in Dayton, supervising radio testing and production.

After graduation in 1926 he began to work at General Motors Radio where he supervised radio testing, and met Robert Mumma, who quickly began a friendship which lasted over 50 years. After supervising the liquidation of General Motors Radio in 1933, he conducted teletype communications research for Telecom Laboratories, a company financed by Charles Kettering of automotive pioneering fame through General Motors and Delco. Two years later he was hired by Harry Williams to be foreman on the Process Laboratory at the Frigidaire Division of General Motors, once again in Dayton. He then followed Williams to the National Cash Register Company in 1938 to form the innovative Electrical Research Laboratory at the direction of Colonel Edward Deeds, then President of the Company.

At Deed's direction he conducted research to implement pioneering ideas regarding the use of tubes and circuitry in counting devices, with the idea of developing high speed mathematical computing machines to augment or replace the Company's mechanical machines. The idea of applying electronic counting to calculating mechanisms occurred to him when reading of a thyratron (gas-filled tube) counting ring of five places (5 digits, not five orders) developed by English scientist Wynn Williams.

42



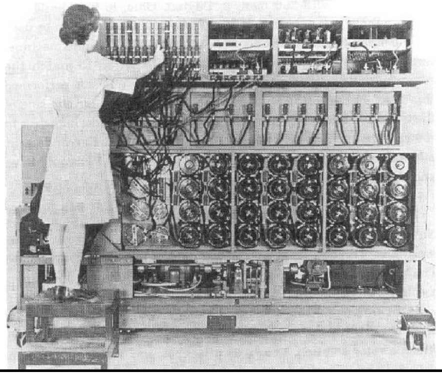
In 1940 his research in the area of computing machines made him prime candidate to evaluate the design for a totally electronic deciphering device created by a group of MIT academics used for codebreaking. While not an expert in cryptanalysis, he gave the opinion that the implementation of the design was not possible, primarily because of the large number of tubes necessary. Believing that the American version of the bombe decryption machine could be built using mechanical and electronic components, and recognizing the NCR Corporation's past accomplishments, the Navy moved ahead with a contract with NCR. In 1943 Desch's team had success in creating their own decoding machine for breaking the Enigma code.

In 1946 Joe filed an application for a patent on an electronic calculator designed by him and Bob Mumma, as part of an application initiated in March of 1940. This brought about three intereferences filed in the US Patent Office between their application and one by Arthur Dickinson of IBM. Eventually these were settled in favor of Desch, in part because he proved Dickinson's design unworkable, and gave Desch and Mumma the first patent on the modern digital computer. His career after this point was noteworthy, and he was especially proud in later years of his work with Bob Mumma in the development of the NCR 304, the first completely solid state computer. He continued to be an integral part of NCR until his retirement in 1972.

For his efforts in building the US bombe he was awarded the Medal of Merit by President Truman in 1947.

43

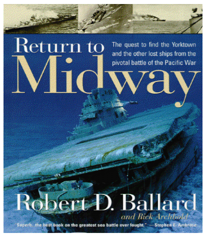
44



45

46

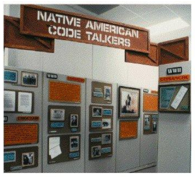
Purple


Return to
Midway
The quest to find the Yorktown and the other lost ships from the pivotal battle of the Pacific War
Robert D. Ballard
and Rick Archbold

- The US broke the Japanese codes early in the war
- Decryptions called *purple*
- Gave much useful information, even about German front!
  - *A weak cipher is worst than no cipher at all*

47

Native American Code Talkers



Surrounded by complex machines, the exhibit on codetalkers appears out of place, but is actually a monument to the most complex machine of all - the human mind. Lacking secure battlefield voice communications during the Great War, the Army employed Choctaws to encrypt voice communications, using their native language, itself encoded.

- Choctaw tribe used in WW I
- Navajo tribe used in WW II
  - *Break it! We can't even transcribe it!*
  - The Japanese never broke the Navajo "code"

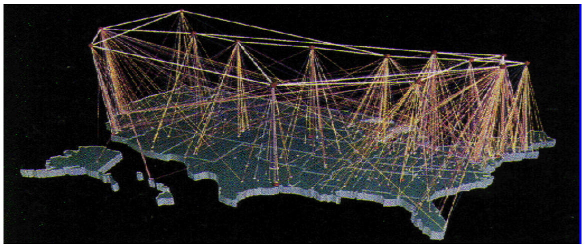
48

The Importance of Cryptography in the Modern World

- Some of the most modern methods of communication are inherently insecure
  - The Internet is very insecure
    - Traffic passes through central hubs
    - Like a giant party line
  - Ethernet networks can have *sniffers*
  - Cable modems pass through other people's homes

49

The Tangled Web We Weave



50

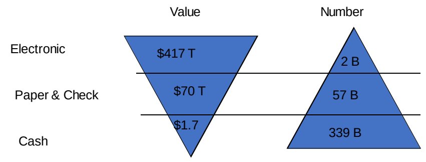
Public Use of Cryptography

- Cryptography is essential for modern e-commerce and standard transactions
- Huge amounts of money move electronically every day
- You can throw away the "green stuff" that you still carry in your pocket
- How can the public use cryptography conveniently (quickly and safely)?

51

US PAYMENTS STRUCTURE 1987

Orders of Magnitude?

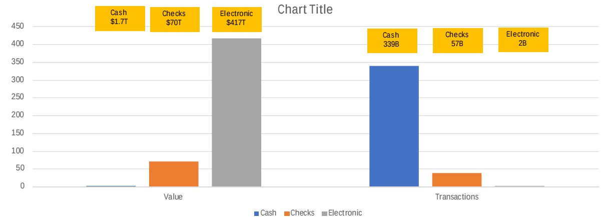


WHAT IS MONEY?

52

US PAYMENTS STRUCTURE 1987

Orders of Magnitude?



53

Transposition Ciphers

- The idea here is to permute the actual letters of the message in some way
- Some examples are:
  - Reverse pairs of letters
    - HELLO WORLD
    - EHLL OOWLRD
  - Remove every second letter and put it at the end.
    - HELLO WORLD
    - HLOWRDEL OL
  - Reverse the letters
    - HELLO WORLD
    - DLROW OLLEH
- Many trickier transpositions are possible

54

Types of Cryptographic Systems

- *Restricted use systems* -- must keep nature of encoding and decoding secret
- *General use systems* -- nature of encoding and decoding is generally known -- must use a *key* to help safeguard system
  - *Secret-key systems* -- most traditional systems -- same key for encoding and decoding
  - *Public-key systems* -- public key provided for encoding and a private key used for decoding

55

Keys and Codes

- A *key* is a small amount of information needed to use a cryptographic system
- For a Caeser type cipher only 26 keys are possible, which is a ridiculously small number.
- For a general substitution cipher, $26! \approx 4*10^{26}$ keys are possible
- Substitution ciphers can easily be broken using frequency analysis

56

The One-Time Pad

- There is one classical provably secure cryptographic system called the *one-time pad*
- As the name suggests, you can only use it once and then it must be replaced
- Very secure, but not very handy
- Uses the xor operator $\oplus$

57

The One-Time Pad

- Recall that $0\oplus0 = 0$, $0\oplus1 = 1$, $1\oplus0 = 1$, and $1\oplus1 = 0$
- Like +, $\oplus$ is commutative ($a \oplus b = b \oplus a$) and ($a \oplus (b \oplus c) = (a \oplus b) \oplus c$).
- In addition, $(a \oplus b) \oplus a = b$
- Makes $\oplus$ handy for computer graphics -- i.e., xoring something to itself cancels it out

58

The One-Time Pad

- The idea here is that if you have a one-time pad and a message, then the sender sends Message $\oplus$ OTP
- The receiver then does (Message $\oplus$OTP) $\oplus$OTP = Message $\oplus$(OTP $\oplus$OTP) = Message
- If the pad is used twice it is possible to deduce what it is

59

The One-Time Pad

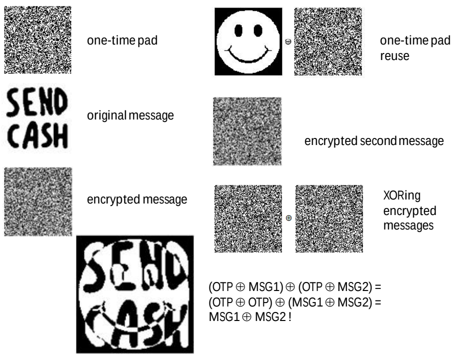
- Why is the one-time pad unbreakable if used only once?
- Because, for any string S and message M of the same length as M, there is a one-time pad Q, such that $M \oplus Q = S$
  - *Proof:* Let $Q = M \oplus S$!
- Why don't we just use one-time pads all the time?
- Was used on the hotline between US and USSR

60

One-Time Pad Reuse

- Don't Do It!
- Why not?
- The following graphical example comes from
- https://cryptosmith.com/2008/05/31/stream-reuse/

61



(OTP ⊕ MSG1) ⊕ (OTP ⊕ MSG2) =
(OTP ⊕ OTP) ⊕ (MSG1 ⊕ MSG2) =
MSG1 ⊕ MSG2 !

62

Problems with Keys

- Distribution
- Updating
- Security
- Distribution
- Updating
- Security
- How can the public use cryptography?

63

Venona Project – Wikipedia

The Venona project (1943–80) was a counter-intelligence program initiated by the U.S. Army's Signal Intelligence Service (later the National Security Agency). The purpose of the Venona project was the decryption of messages transmitted by the intelligence agencies of the Soviet Union, e.g. the NKVD, the KGB (foreign intelligence) and the GRU (military intelligence). During the 37-year duration of the Venona project, the Signal Intelligence Service decrypted and translated approximately 3,000 messages from Russian to English; among the signals-intelligence yielded was discovery of the Cambridge Five espionage ring in Britain and Soviet espionage of the Manhattan Project in the U.S. The Venona project remained secret for more than fifteen years after it concluded, and some of the decoded Soviet messages were not declassified and published until 1995.

64

Venona Project – Wikipedia

This message traffic, which was encrypted with a one-time pad system, was stored and analyzed in relative secrecy by hundreds of cryptanalysts over a 40-year period starting in the early 1940s. Due to a serious blunder on the part of the Soviets, some of this traffic was vulnerable to cryptanalysis. The Soviet company that manufactured the one-time pads produced around 35,000 pages of duplicate key numbers, as a result of pressures brought about by the German advance on Moscow during World War II. The duplication—which undermines the security of a one-time system—was discovered and attempts to lessen its impact were made by sending the duplicates to widely separated users. Despite this, the reuse was detected by cryptologists in the US.

65

Venona Project – Wikipedia

The decrypted messages gave important insights into Soviet behavior in the period during which duplicate one-time pads were used. With the first break into the code, Venona revealed the existence of Soviet espionage at Los Alamos National Laboratories. Identities soon emerged of American, Canadian, Australian, and British spies in service to the Soviet government, including Klaus Fuchs, Alan Nunn May, and Donald Maclean. Others worked in Washington in the State Department, the Treasury, Office of Strategic Services, and even the White House.

The decrypts show the U.S. and other nations were targeted in major espionage campaigns by the Soviet Union as early as 1942. Among those identified are Julius and Ethel Rosenberg; Alger Hiss; Harry Dexter White, the second-highest official in the Treasury Department; Lauchlin Currie, a personal aide to Franklin Roosevelt; and Maurice Halperin, a section head in the Office of Strategic Services. CHECK ALSO NSA.GOV

66