Hardy's Mistake
The Unexpected Applicability of Pure Mathematics to Cryptography

Spring 1996 G. C. Steward Lectures
Gonville and Caius College

Whitfield Diffie
Sun Microsystems

1 March 1996

1

A Note from Our Sponsor

I begin by laying stress on the *harmlessness* of mathematics — 'the study of mathematics is, if an unprofitable, a perfectly harmless and innocent occupation'.

G. H. Hardy
A Mathematician's Apology
1940

2

A Note from Our Sponsor — bis

There is one comforting Conclusion which is easy for a real mathematician. Real mathematics has no effects on war. No one has yet discovered any warlike purpose to be served by the theory of numbers or relativity, and it seems very unlikely that anyone will do so for many years.

G. H. Hardy
A Mathematician's Apology
1940

3

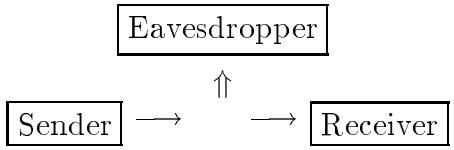
A Note from Our Sponsor — ter

I do not know what is the hightest degree of accuracy which is ever useful to an engineer — we shall be very generous if we say ten significant figures.

G. H. Hardy
A Mathematician's Apology
1940

4

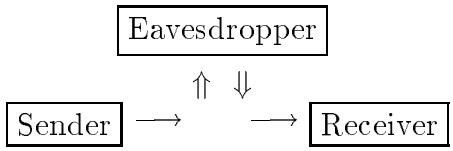
Privacy or Confidentiality



Guarantee to Sender
Authorized Receivers Only

5

Authenticity and Integrity



Guarantee to Receiver

- Knows Identity of Sender
- Message Not Altered
- Not Unduly Delayed

6

Cryptographic System

Plain Text Space $\longrightarrow$ $\{\mathcal{S}_k\}_{\{k\}\in\mathcal{K}}$ Cipher Text Space

7

Vigenère Table

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	Q	F	A	L	H	I	M	Z	E	T	Y	N	B	O	U	D	X	P	C	S	K	G	R	J	V	W
B	Y	L	K	O	R	U	C	J	X	P	A	S	V	H	B	D	Q	G	M	I	T	E	Z	J	W	N
C	J	O	A	M	S	I	T	Y	R	D	N	H	X	E	W	P	F	V	Z	B	L	G	K	Q	U	C
D	B	H	X	I	E	W	L	P	C	R	V	A	F	T	S	M	U	N	Q	K	Z	D	G	O	Y	J
E	O	E	N	F	G	D	H	Z	J	B	R	I	S	Y	V	W	T	X	U	L	P	K	Q	A	C	M
⋮																										

8

Effect of Vigenère

Plain:	d	o	d	e	c	a	h	e	d
	B ↓	*A* ↓	*D* ↓	*C* ↓	*A* ↓	*D* ↓	*B* ↓	*A* ↓	*D* ↓
Cipher:	O	U	I	S	A	B	J	H	I

'd' is carried to 'O' under the 'B' alphabet; 'o' is carried to 'U' under the 'A' alphabet; 'd' is carried to 'I' under the 'D' alphabet; etc.

9

Vigenère with Cyclic Substitution

Plain:	`HENRY IS HUNGRY ...`
Key:	`PAPAD UM PAPADU ...`
Cipher:	`WECRB CE WUCGUS ...`

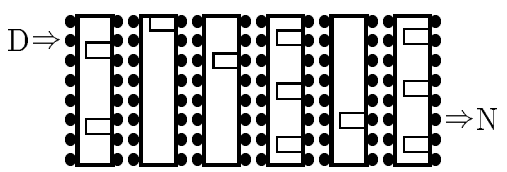
10

Double Vigenère System

Plain:	`HENRY IS HUNGRY ...`
Key-1:	`PAPAD UM PAPADU ...`
Cipher-1:	`WECRB CE WUCGUS ...`
Key-2:	`HIPSH IP SHIPSH ...`
Cipher-2:	`DMRJI KT OBKVMZ ...`

11

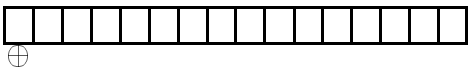
Rotor Machine



Stepping Mechanism

12

Nonlinear Shift Register



Feedback Function

13

Virtues of Cryptography

- Only known way of protecting communication on a channel that is out of the control of the sender and receiver.
- Cost is independent of the length or shape of the path the message follows.

14

Unique Vice of Cryptography

Breaches of cryptosecurity can reach backward in time to expose messages sent earlier.

15

Key Distribution

Private Message Requires Unique Key

- 100 subscribers need 10,000 keys.
- Secret keys must be protected.

16

Key Distribution Process

A. A calls KDC prior to calling B.
B. KDC sends A a certificate: a dated message containing the key with a part A can read and a part B can read.
C. A and B can now communicate.
D. A and B may cache the key for later use.

17

Digital Signatures

Settle Disputes
Between Sender and Receiver

- Only One Person Can Produce It
- Anyone Can Recognize It

18

Public Key Cryptography

- Keys Come In Inverse Pairs
- Given One — Can't Find the Other

19

Fundamental Property

Public Key
— In telephone directory

Secret Key
— In subscriber's safe

20

Signed and Sealed Message

Sealed

$$\Big\{ \{message\}^{\text{Sender Private Key}}, SenderID \Big\}^{\text{Receiver Public Key}}$$

Signed

21

Oneway Functions

- Easy to Compute Forward
- Hard to Go Back

22

Easy to Multiply

$127 \times 997 = 126,619$

Hard to Factor

$126,619$

23

Easy to Raise Numbers to Powers

$x \to x^y$

Hard to Extract Roots

$x \to \sqrt[y]{x}$

Hard to Take Logarithms

$x \to \log_x y$

24

Trapdoor Oneway Functions

- Looks Like Oneway Function
- Designer Knows How to Invert

25

Exponential Key Agreement

Choose a large prime P and a primitive element α in arithmetic modulo P (I.e., $\forall_{0<n<P}\exists k$ such that $\alpha^k = n \pmod P$ or the α^n generate all non-zero elements of GF(P).)

For any $x \in$ GF(P) calculating α^x mod P is easy, but given that $\alpha^x = y \pmod P$, finding $x = \log_\alpha \pmod P$ is hard.

26

Exponential Key Agreement (Cont'd)

A and B want to communicate.

A generates x at random and sends α^x to B.
B generates y at random and sends α^y to A.
A calculates $(\alpha^y)^x = \alpha^{xy}$.
B calculates $(\alpha^x)^y = \alpha^{xy}$.
A and B now both know α^{xy}.

27

RSA* System

$$Message \rightarrow Message^{\mathrm{e}} \pmod{p \times q}$$

Public Key is Product $p \times q$

Secret Key is Factors: (p, q)

* Rivest, Shamir, and Adleman

28