

①

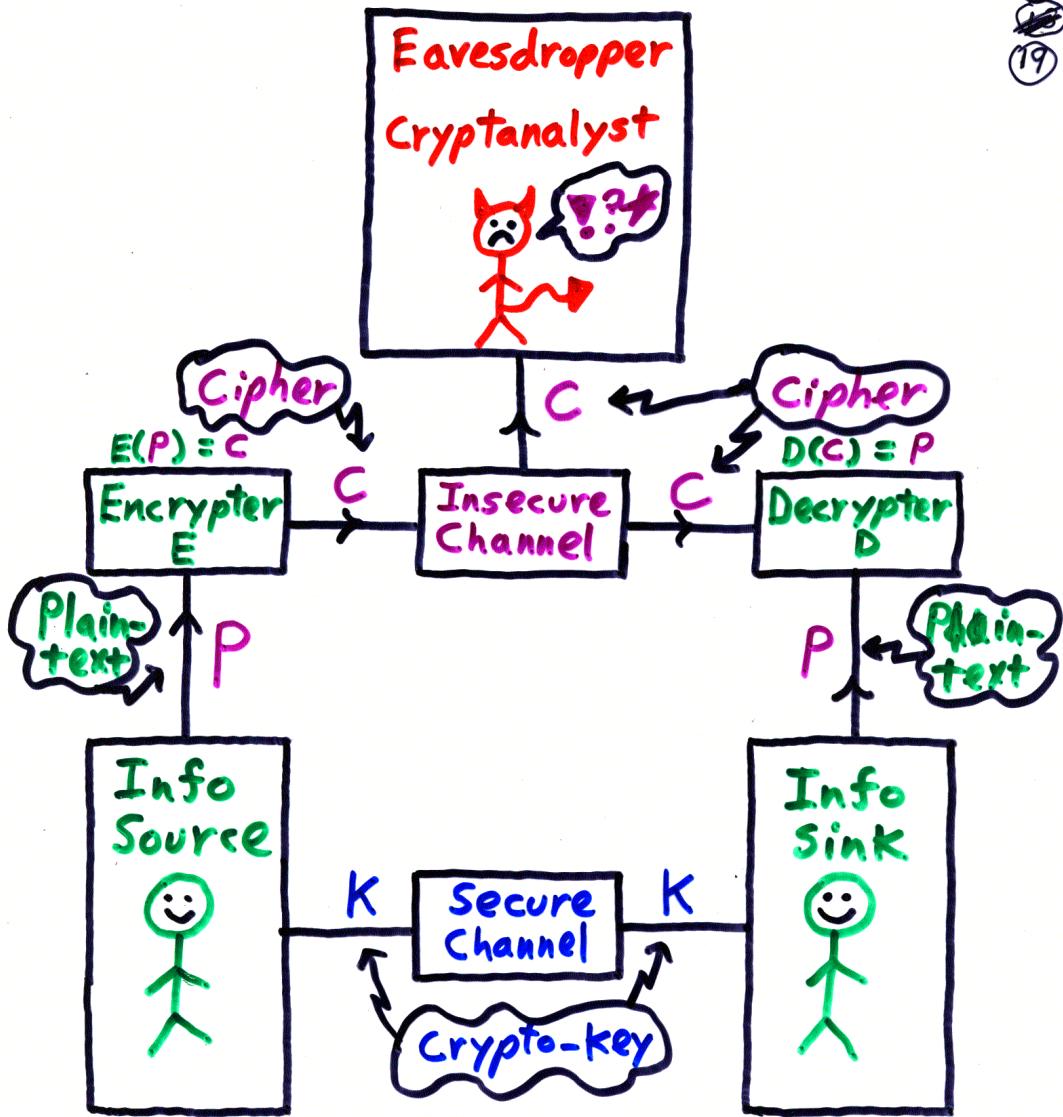
# PUBLIC-KEY CRYPTOSYSTEMS

in

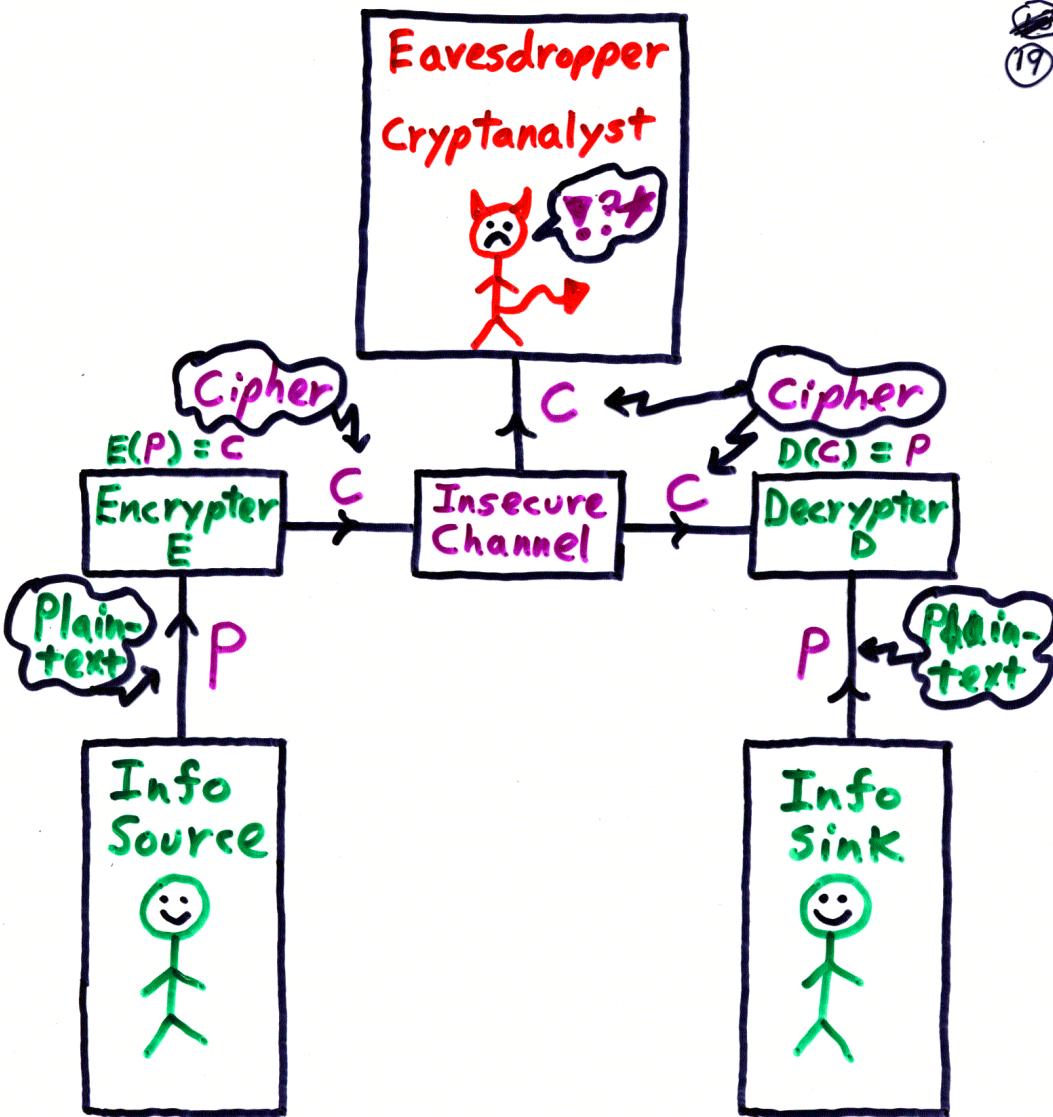
Computer Color

and in

Synchronous Sound



Conventional Cryptosystem  
 (Shannon, Bell. Sys. Tech. J. (1949))



# Conventional Cryptosystem

Plaintext  $P$

$P = \text{YOU RECENTLY...}$

Conv.  $\text{blank} = 00, A = 01, B = 02, \dots, Z = 26$

$P = \text{YOU RECENTLY...}$   
25 15 21 00 18 05 03 05 14 20 12 25 ...

$P = \boxed{\text{RECENTLY}}$  2100 1805 0305 1420 ...  
25 15

$P = P_1 \quad P_2 \quad P_3 \quad P_4 \quad P_5 \quad \dots$

Plaintext

(5)



$$D(C) = P$$

or  $D(C_i) = P_i$

---

$$D(E(P)) = P$$

(6)

## Obj. of Cryptosystem :

### Unconditional Security

i.e., Must be impervious  
to cryptanalytic attack  
even if cryptanalyst has

- Cryptosystem equipment
- Unlimited Cipher
- Unlimited plaintext/cipher pairs

7

## Cryptanalyst Attacks

- 1) Cipher text only attack  $\equiv$   
 $C$  Known
- 2) Known Plaintext attack  
 $(P, C)$  Known
- 3) Chosen Plaintext attack  
 $(P, C)$  Known  
chosen  $\nearrow$

### Example. 1

One Time  
Pad

(Unconditionally Secure)

Key =  $K = R_1 R_2 \dots R_n \dots$  Seq. of Random Nos.

### Encrypting Algorithm

$$C_i = P_i + R_i \pmod{26}$$

where  $\pmod{26}$  means:

remainder after division by 26

E.G.,  $C_i = P_i + R_i = 13 + 22 = 35 = 9 \pmod{26}$

$$\begin{array}{r} 1 \\ 26 \overline{)35} \\ \underline{26} \\ 9 \end{array}$$

Remainder

(7)

Problem: Long random number seg. must be sent over secure channel

---



---

Pitfall: If one time pad is used more than once, then cipher can easily be broken !

$$\left. \begin{array}{l} C_i = P_i + R_i \\ C_{i+n} = P_{i+n} + R_i \end{array} \right\} \Rightarrow C_{i+n} - C_i = P_{i+n} - P_i \pmod{26}$$


---

But  $P_{i+n} - P_i$  is so far from random that its statistical fingerprint can be used to crack the cipher

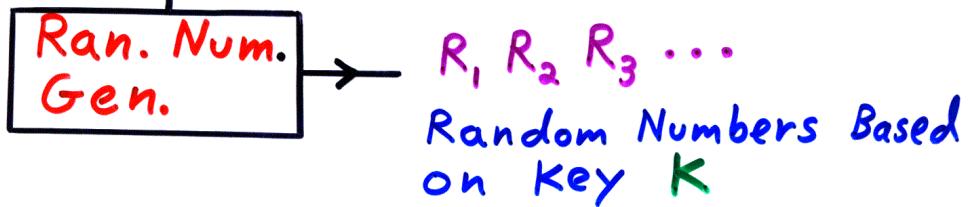
(10)

Example. 2

## Random Number Generator Seed

Initializing  
Key

K



$$C_i = P_i + R_i \pmod{26}$$

Advantage: Only small key K needs to be sent over secure channel

Disadvantage: Loss of Security

## Substitution Cipher

Example. 3

E.G., Caesar Cipher

Key = fixed integer  $K$

$$0 < K < 26$$

$$C_i = P_i + K \pmod{26}$$

---

Advantage: Only small Key need be sent over secure channel

---

Disadvantage: Can easily be broken because plaintext has a statistical fingerprint which is far from random.

## Caesar Cipher

$$C_i = P_i + K \pmod{36}$$

A B C D E F G H I J K L M N O P O R

0 1 2 3 4 5 6 7 8 9 A B C D E F G H

S T U V W X Y Z 0 1 2 3 4 5 6 7 8 9

I J K L M N O P Q R S T U V W X Y Z

$$\text{key} = K = 10$$

(13)

Example . 4

## Permutation Cipher

Reshuffle letters in  
message in a fixed way,  
i.e., by a fixed permutation  $\pi$

E.G.,

	RECENTLY	...
1 2 3 4	1 2 3 4	...
↓	↓	...
3 4 2 1	3 4 2 1	...
C EER	LYTN	...

(14)

Advantage: Only a small key  
be sent over  
secure channel,  
namely,  $\Pi$

---

Disadvantage: Can easily be  
broken because  
permutation  
not strong  
enough to  
destroy  
statistical  
fingerprint  
of plaintext

## Other Ciphers

Combinations of

- Permutation Ciphers
- Substitution Ciphers
- Random No. Gen.

Mind Boggling !

{ comp. sci.  
Math.  
linguistics

(16)

## Obj. of Cryptosystem : Safety

### Old Idea :

#### Unconditional Security

The system can resist any cryptanalytic attack no matter how much computation is involved.

New Idea:



## Computational Security

System is secure because of the computational cost of cryptanalysis, but would succumb to an attack with unlimited computation.

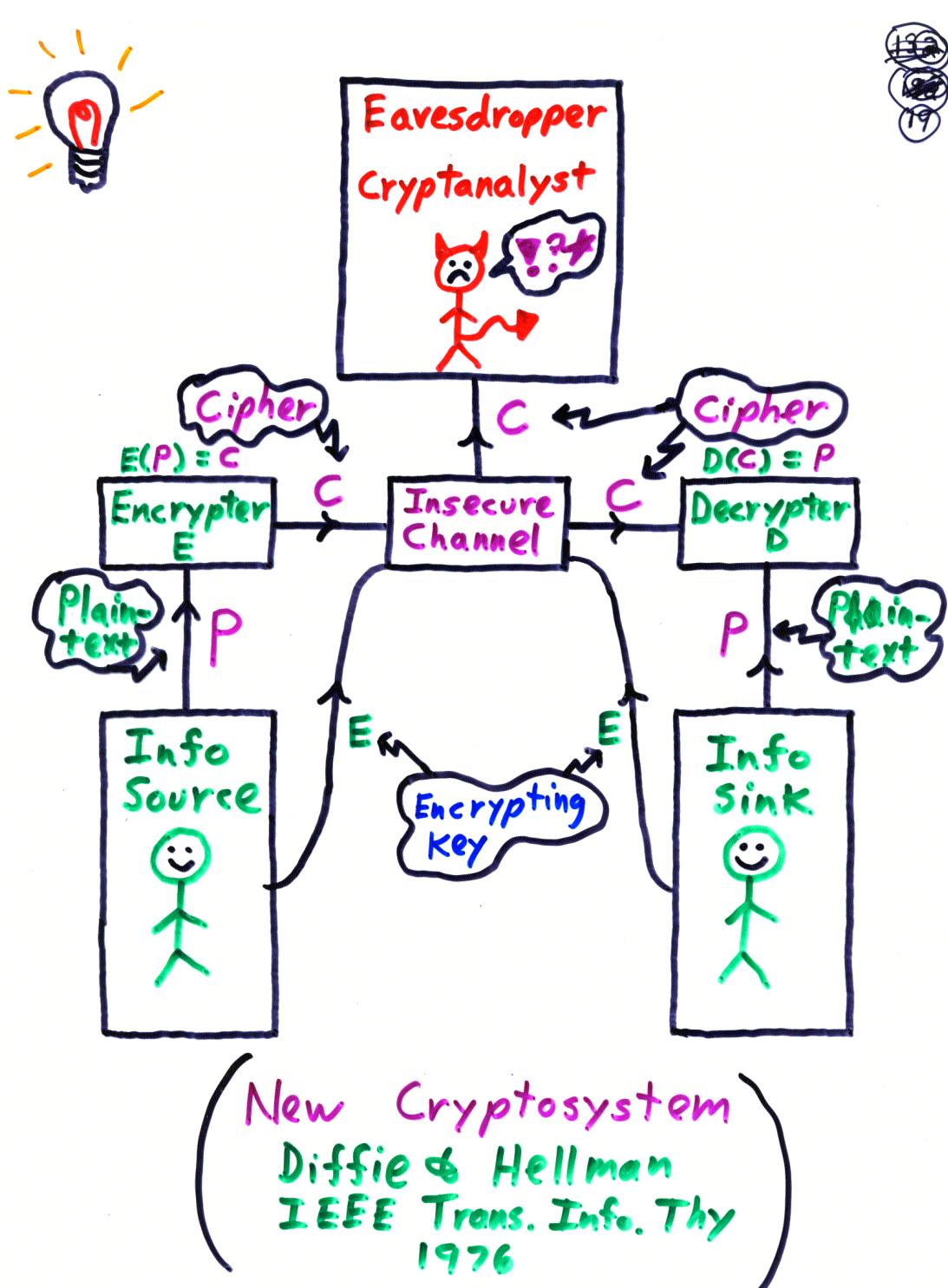
### For Example:

- a) Requires  $10^{30}$  years  
to break on the  
fastest known computer
- b) or, requires  $10^{100}$  bits  
of memory to break
- c) or, requires  $10^{30}$  dollars  
to break

System computationally safe  
implies safe for all  
practical purposes

Idea comes from new  
field in comp. sci.

Computational  
complexity



New idea



Revealing E

20

Does not reveal D !

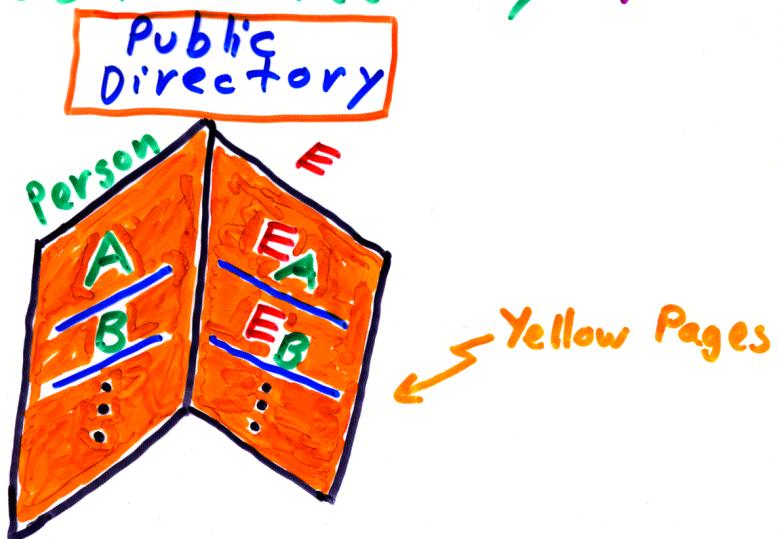
E can be chosen so that  
it is computationally impossible  
to compute  $D = E^{-1}$  from E.

Such an E is called a  
Trap Door Function.



## New idea (cont.)

Therefore, why doesn't everyone publish his encrypting key  $E$  in a public directory?



Thus, a Public-key Cryptosystem is born !

## Ground Rules For: PKCS

(22)

Each person A chooses an encrypting transf.  $E_A$  and a decrypting transf.  $D_A$  such that:

- $\underline{D_A(E_A(P)) = P}$
- Both  $E_A$  and  $D_A$  are "easy" to compute
- $D_A$  is hard to compute from  $E_A$  (i.e.,  $E_A$  is a trap door function)
- $\underline{E_A(D_A(P)) = P}$

## PKCS (Cont.)

If A wishes to send a message P to B, A looks up  $E_B$  in the public directory (yellow pages) and then sends:

$$C = E_B(P)$$


---

Only B can decipher C, for only he (or she) knows  $D_B$ . Hence B can apply  $D_B$  to recover:

$$P = D_B(C) = D_B(E_B(P))$$

(24)

New Idea:



## Signatures

A message  $P$   
from A to B can be  
unequivocally signed  
by A !

(25)

A signs message to B  
as follows:

---

• A sends  $C = E_B D_A(P)$

---

- B receives C and deciphers by:

$$E_A D_B(C) = \underline{E_A D_B(E_B D_A(P))} = P$$

---

- B knows that A signed the message for only A knows  $D_A$
- 

Receiver B thereby knows sender is A

(26)

## Example: (a Poor) PKCS

Represent plaintext  $P$  as an  $n$ -vector, i.e.:

$$P = (P_1, P_2, \dots, P_n)$$

E.G.,  $P = (2, 23, 0, 5, \dots, 13)$

Let  $E_A$  be mult. by a matrix  $M_A$ , i.e.,

$$C = E_A(P) = P \cdot M_A$$

Easy  
 $n^2$   
steps

Hence,  $D_A$  is mult. by the matrix  $M_A^{-1}$ , i.e.,

$$P = D_A(C) = C \cdot M_A^{-1}$$

Easy  
 $n^2$   
steps

However, given  $E_A$  (i.e., given  $M_A$ ), the decrypting transformation  $D_A$  (i.e.,  $M_A^{-1}$ ) is harder to find. It takes many more than  $n^2$  steps to find  $M_A^{-1}$

Unfortunately,  $D_A$  can still be computed from  $E_A$  with a reasonable amount of effort. Hence, system is not practical.

(28)

Digression: Some Needed  
Number Theory

Def. A prime is a pos. number ( $\neq 1$ ) exactly divisible only by 1 and itself.

Examples of primes: 2, 3, 5, 7, 11, ...

Examples of non-primes: 4, 6, 8, 9, 10, ...

Theorem: Every pos. integer can be uniquely factored into a product of primes.

Examples:  $6 = 2 \cdot 3$   
 $12 = 2 \cdot 2 \cdot 3$   
 $90 = 2 \cdot 3 \cdot 3 \cdot 5$

Def. The greatest common divisor of two integers  $a$  and  $b$ , written:

$$\gcd(a, b)$$

is the largest pos. integer which exactly divides both  $a$  and  $b$ .

Examples:  $\gcd(6, 4) = 2$

$$\gcd(2, 3) = 1$$

$$\gcd(12, 30) = 6$$

Def. Two integers  $a$  and  $b$  are relatively prime if

$$\gcd(a, b) = 1$$

## Modular Arith Arith Modulo An Integer $n$ (30)

$a = b \pmod{n}$  iff  $a - b$  is exactly divisible by  $n$ , i.e., there exists an integer  $\lambda$  such that  $a - b = \lambda n$ .

### Examples:

$$a - b = \lambda \cdot n$$

$$5 = 2 \pmod{3}, \text{ for } 5 - 2 = 1 \cdot 3$$

$$13 = 7 \pmod{2}, \text{ for } 13 - 7 = 3 \cdot 2$$

$$3 = 18 \pmod{5}, \text{ for } 3 - 18 = (-3) \cdot 5$$

(31)

Fact " $\equiv (\text{mod } n)$ " behaves like ordinary " $=$ " except every integer is " $\equiv (\text{mod } n)$ " to exactly one of the integers:

$$0, 1, 2, \dots, n-1$$

Fact " $\equiv (\text{mod } n)$ " behaves like " $=$ " when working with addition, subtraction, multiplication, powers, etc.

Examples:

$7+6 \equiv 3 \pmod{10}$
$7 \cdot 6 \equiv 9 \pmod{11}$

Examples:

Compute $2^4 \pmod{5}$
$2^2 \equiv 4 \pmod{5}$
$2^3 \equiv 8 \equiv 3 \pmod{5}$
$2^4 \equiv 6 \equiv 1 \pmod{5}$

(32)

Theorem Given integers  
e and n

such that:

$$\gcd(e, n) = 1,$$

Then there exists an integer  
d

unique modulo n such that

$$e \cdot d = 1 \pmod{n}$$

# PKCS (Rivest et al, 1977)

## Method:

- Choose large primes  $p$  and  $q$
- Choose a large integer  $e$  such that:

$$\gcd[e, (p-1) \cdot (q-1)] = 1$$

- Let  $n = p \cdot q$

- Then there exists a unique integer  $d \bmod (p-1) \cdot (q-1)$  such that:

$$\begin{cases} ed = 1 \bmod (p-1) \cdot (q-1) \\ \text{and} \\ \gcd[d, (p-1) \cdot (q-1)] = 1 \end{cases}$$

27

## Encryption

$$C = E(P) = P^e \pmod{n}$$

$\therefore (e, n)$  is the encryption key

Place  $(e, n)$  in the  
Public Directory

## Decryption

$$P = D(C) = C^d \pmod{n}$$

$\therefore (d, n)$  is the decryption key

Conceal d

Observation:  $E$  and  $D$  satisfy the four properties for a Public-key Cryptosystem, i.e.,

(1)  $D(E(P)) = P$

(2) Both  $E$  and  $D$  are "easy" to compute

(3)  $D$  is "hard" to compute from  $E$  (i.e.,  $E$  is a trapdoor function)

(4)  $E(D(P)) = P$

(36)

E is a trapdoor function,  
i.e.,  $(d, n)$  is "hard" to  
compute from  $(e, n)$ . For:

Theorem Computing  $d$  from  
 $e$  and  $n$  is equivalent to  
factoring  $n = p q$

Fact Factoring is exceedingly  
computationally hard.

Thus we have a PKCS where each user  $X$  selects:

(a) An encryption key

$$E_X = (e_X, n_X)$$

(b) And a decryption key

$$D_X = (d_X, n_X)$$

as directed above. Each user  $X$  places  $E_X$  in the public directory But keeps  $D_X$  secret.

---

If each user chooses  $p$  and  $q$  to be 100 digit long random primes, then it is not computationally possible to compute  $d$  from  $(e, pq)$ .

For assuming  $10^{-3}$  seconds per instruction, it would take  $3.8 \times 10^9$  years to factor  $pq$  !

On the other hand, encrypting and decrypting only take a few seconds of computer time.

Implementation

SOON

(39)

On one NMOS chip

$n \approx 500$  bits  $\approx 150 - 160$  digits

$p$  and  $q \approx 250$  bits  $\approx 80$  digits

Data Rate: Approximately  
1200 baud

Data Rate theoretical limit  
using bipolar logic  
20,000 bits/sec.

Caveat: There is no mathematical  
proof that factorization  
is exceedingly hard.

(40)

Example Scientific Amer., 1977  
(Rivest et al.)

Choose:  $p = 47$  (a prime)

$q = 59$  (" ")

$$\therefore n = pq = (47)(59) = 2773$$

$$d = 157$$

$$\therefore (p-1)(q-1) = (46)(58) = 2668$$

$$\therefore e = 17$$

where

$$ed = (17)(157) = 1 \pmod{2668}$$

Consider the plaintext:

$P = \text{ITS ALL GREEK TO ME.}$

(Julius Caesar, I, ii, p 288, paraphrased)

---

Let

blank = 00, A = 01, B = 02, ..., Z = 26

Then the plaintext becomes:

$P_1$	$P_2$	$P_3$	$P_4$	$P_5$
0920	1900	0112	1200	0718
0505	1100	2015	0013	0500
$P_6$	$P_7$	$P_8$	$P_9$	$P_{10}$

(42)

The cipher is computed as follows:

$$C_1 = E(P_1) = P_1^{17} = 948 \pmod{2773}$$

:

.

$$\begin{array}{cccccc} C = & 0948 & 2342 & 1084 & 1444 & 2663 \\ & 2390 & 0778 & 0774 & 0219 & 1615 \end{array}$$


---

Decrypting,

$$P = D(C)$$

$$\begin{aligned} D(C_1) &= D(0948) = 948^{157} \\ &= 920 \pmod{2773} \end{aligned}$$


---

(+3)

W I N

---

---

\$ 100

---

---

Martin Gardner  
Scientific American  
August, 1977

## Break the following:

$$E = (\textcolor{red}{e} \mod n)$$

$$\textcolor{red}{e} = 9007$$

$n = 11438162575738837669235779976146612010213296721242362562$  ETC.

$$n = pq$$

P 64 DIGITS

Q 65 DIGITS

FIND  $\textcolor{red}{d}$  AND CRACK THE CIPHER ON PAGE 121, I.E.,

9636	9613	7546	2206
1477	1409	2225	4355
8829	0575	9991	1245
7431	9374	6951	2093
0816	2982	2514	5708
3569	3147	6622	8839
8962	3013	3919	9055
1829	9451	5781	5154

SIGNED,

16717861150380344246015271389168393245436901, ETC

= D (FIRST SOLVER WINS ONE HUNDRED DOLLARS)