Great Theoretical Ideas In Computer Science

S. Rudich
V. Adamchik

CS 15-251 Spring 2006

Lecture 8 Feb. 09, 2006 Carnegie Mellon University

RSA Cryptosystem

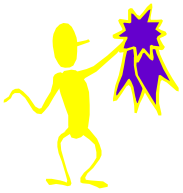
$=_p 1$

Cryptography

Cryptography is the mathematics of devising secure communication systems

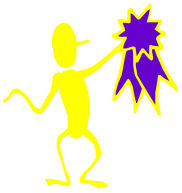
Cryptanalysis is the mathematics of breaking such systems.

RSA Cryptography



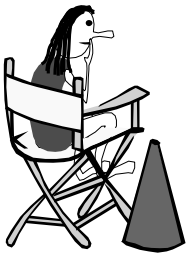
Basically unbreakable method for encoding messages

RSA Cryptography

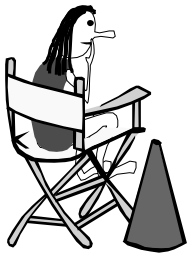


Rivest
Shamir
Adelman
(1978)

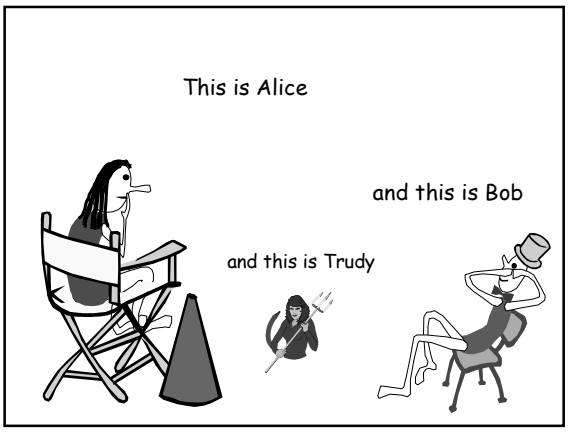
This is Alice

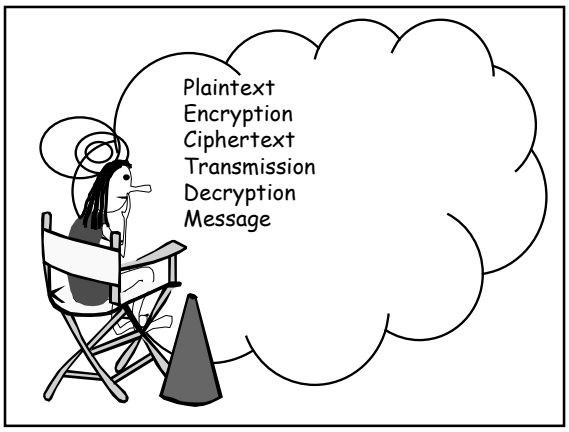


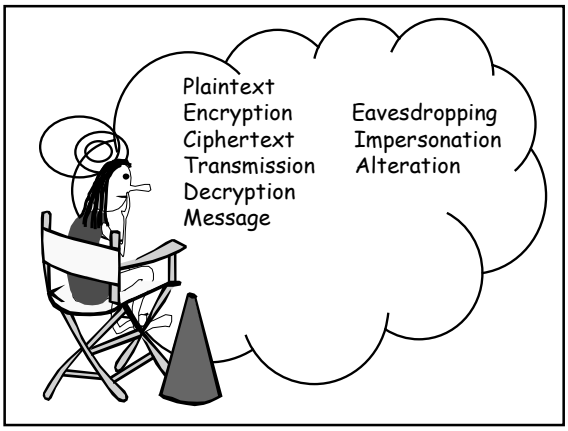
This is Alice

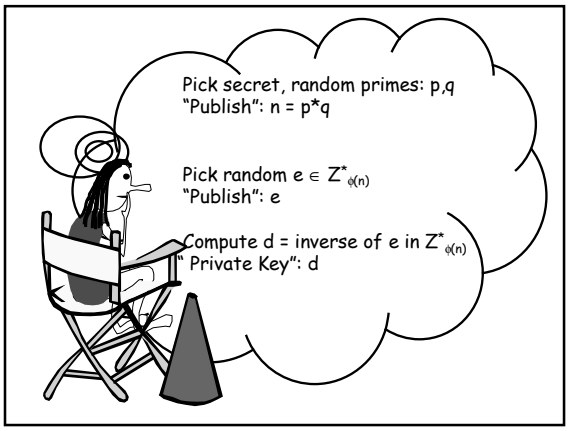


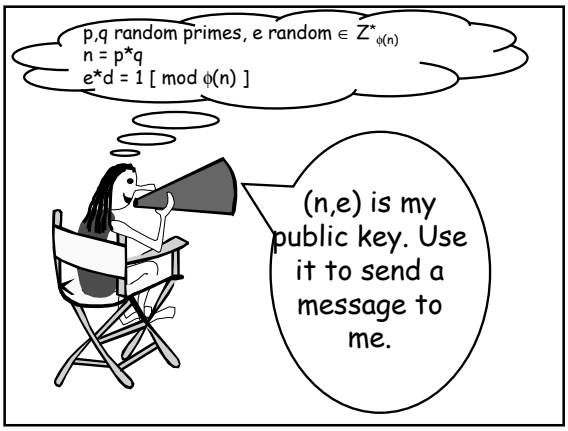
and this is Bob

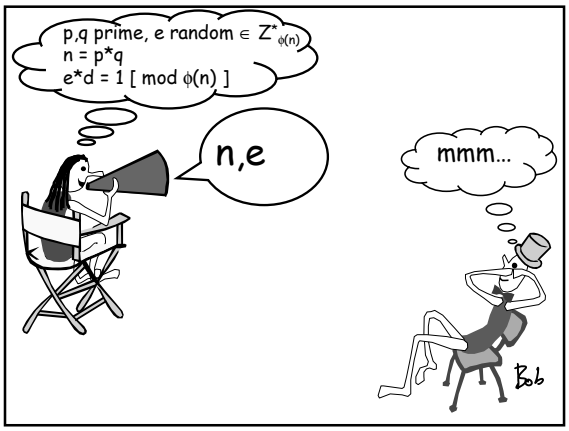

This is Alice
and this is Bob
and this is Trudy

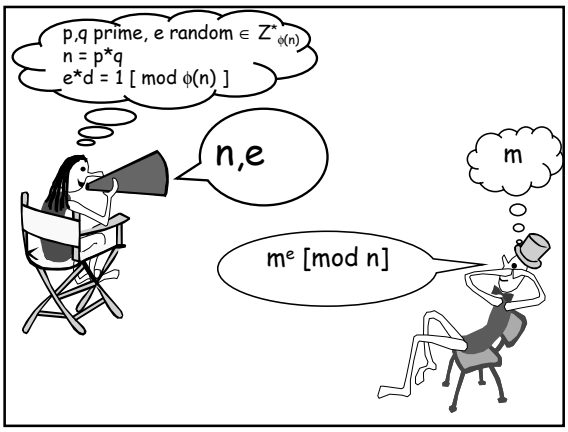

Plaintext
Encryption
Ciphertext
Transmission
Decryption
Message

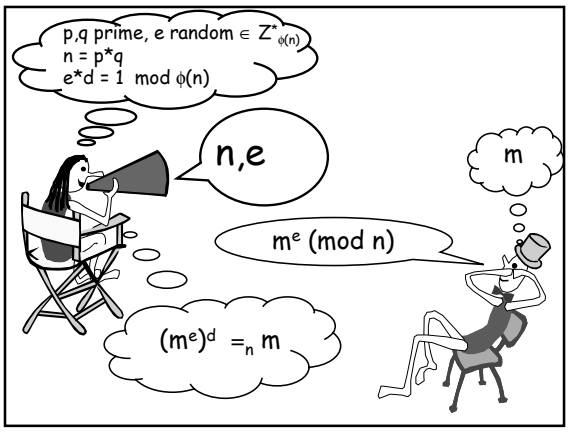

Plaintext
Encryption
Ciphertext
Transmission
Decryption
Message
Eavesdropping
Impersonation
Alteration


Pick secret, random primes: p,q
"Publish": n = p*q
Pick random e ∈ Z*φ(n)
"Publish": e
Compute d = inverse of e in Z*φ(n)
" Private Key": d


p,q random primes, e random ∈ Z*φ(n)
n = p*q
e*d = 1 [mod φ(n)]
(n,e) is my public key. Use it to send a message to me.


p,q prime, e random ∈ Z*φ(n)
n = p*q
e*d = 1 [mod φ(n)]
n,e
mmm...
Bob





RSA Example

n = 187=11*17
e = 7

S	M	I	L	E	Y
19	13	09	12	05	25

RSA Example

n = 187=11*17
e = 7

S	M	I	L	E	Y
19	13	09	12	05	25

19^7=145 mod 187
13^7=106 mod 187

RSA Example

n = 187=11*17
e = 7

	S	M	I	L	E	Y
m	19	13	09	12	05	25
m^e mod n	145	106	70	177	146	185

RSA Example

n = 187=11*17
e = 7

	S	M	I	L	E	Y
m	19	13	09	12	05	25
m^e mod n	145	106	70	177	146	185
m^{e*d} mod n						

RSA Example

n = 187=11*17
e = 7

	S	M	I	L	E	Y
m	19	13	09	12	05	25
m^e mod n	145	106	70	177	146	185
m^{e*d} mod n						

d = 23

RSA Example

n = 187=11*17
e = 7

	S	M	I	L	E	Y
m	19	13	09	12	05	25
m^e mod n	145	106	70	177	146	185
m^{e*d} mod n						

d = 23

$145^{23}=19 \bmod 187$

RSA Cryptography

Fast Exponentiation
Extended Euclidean Algorithm
Modular inverses
FLT (Fermat's Little Theorem)
CRT (Chinese Remainder Theorem)

Fast Exponentiation

How to compute

$$1911^{2396} \bmod 4171$$

fast?

Fast Exponentiation

A more lucid example

$3^{50} \bmod 7$

$50 = 110010_2$

$3^{50} = ((((3^2 *3)^2)^2)^2 *3)^2$

Fast Exponentiation

A more lucid example

$3^{50} \bmod 7$

$((((3^2 *3)^2)^2)^2 *3)^2 = ((((2 *3)^2)^2)^2 *3)^2 =$

$(((36)^2)^2 *3)^2 = ((1)^2 *3)^2 = 3^2 = 2 \bmod 7$

Modular Inverses

Definition
The inverse of e mod n is

$$d*e = 1 \bmod n$$

Modular Inverses

Definition
The inverse of e mod n is

$$d*e = 1 \bmod n$$

Question.
What is the inverse of 3 mod 29?

Modular Inverses

Definition
The inverse of e mod n is

$$d*e = 1 \bmod n$$

Question.
What is the inverse of 4 mod 8?

Modular Inverses

Definition
The inverse of e mod n is

$$d*e = 1 \bmod n$$

Theorem.
e has an inverse mod n iff GCD(e,n)=1

Modular Inverses

Theorem.
e has an inverse mod n iff GCD(e,n)=1
Proof.
By the EEA

$$1 = a*e + b*n$$

Extended Euclidean Algorithm

The algorithm works the same as the regular Euclidean algorithm, except it keeps track of more details.
It computes x and y such that

$$GCD(a,b) = a*x + b*y$$

Extended Euclidean Algorithm

Application.

Recall the Die Hard movie. Willis and Jackson are supposed to disarm a bomb by measuring exactly 4 gallons of water using only 3 and 5-gallons containers.

GCD(3,5) = 2*3 + (-1)*5

Extended Euclidean Algorithm

$a = b*q_1 + r_1$

$b = r_1*q_2 + r_2$

...

$r_{k-1} = r_k*q_{k+1}+0$

$$\begin{pmatrix} a & 1 & 0 \\ b & 0 & 1 \\ r_1 & 1 & -q_1 \\ r_2 & -q_2 & 1+q_1 q_2 \\ & \cdots & \\ r_k & x & y \end{pmatrix} \begin{matrix} \\ *(-q_1) \\ *(-q_2) \\ *(-q_3) \\ \cdots \end{matrix}$$

Exponential Inverses

How to find d?

$m^{e*d} = m \pmod n$

Fermat Little Theorem

If a does not divide p and p is prime

$a^{p-1} = 1 \pmod p$

$a^p = a \pmod p$

Fermat Little Theorem

$a^{p-1} = 1 \pmod p$

Compute

$9^{100} \bmod 17$

Fermat Little Theorem

$a^{p-1} = 1 \pmod p$

Compute

$9^{100} = 9^{16*6+4}$

$9^{16} = 1 \bmod 17$

$9^{100} = 9^4 = 16 \bmod 17$

Exponential Inverses

FLT:

$a^{p-1} = 1 \pmod{p}$

Exercise.

$m^{3*d} = m \pmod{11}$

Exponential Inverses

FLT:

$a^{p-1} = 1 \pmod{p}$

Exercise.

$m^{3*d} = m \pmod{11}$

Wrong d: $3*d = 1 \pmod{11}$

Exponential Inverses

FLT:

$a^{p-1} = 1 \pmod{p}$

Exercise.

$m^{3*d} = m \pmod{11}$

$3*d = 1 \pmod{10}$

$m^{1+10*k} = m \pmod{11}$

Exponential Inverses

How to find d?

$m^{e*d} = m \pmod{n}$

We found that d must be inverse of e mod (n-1)

$m^{1+k*(n-1)} = m \pmod{n}$

Exponential Inverses

$m^{e*d} = m \pmod{n}$

We found that d must be inverse of e mod (n-1)

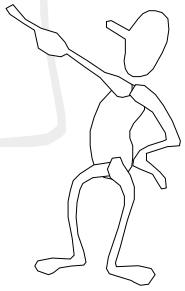
$d*e = 1 \pmod{n-1}$

This idea will make trivial to decrypt messages…

RSA uses

n = p*q

a product of two primes



Exponential Inverses

Theorem.
e, p and q are primes and
GCD(e, (p-1)(q-1)) = 1
Then exponential inverse of e is the inverse of e mod (p-1)(q-1)

$d*e = 1 \bmod (p-1)(q-1)$

Exponential Inverses

Theorem.
$d*e = 1 \bmod (p-1)(q-1)$
Example.
Let n = 5*7. Find d.
$m^{d*5} = m \pmod n$

Exponential Inverses

Theorem.
$d*e = 1 \bmod (p-1)(q-1)$
Example.
Let n = 5*13. Find d.
$m^{d*5} = m \pmod n$
$d*5 = 1 \bmod (4*12)$
d = 29
$m^{145} = m \pmod{65}$

Exponential Inverses

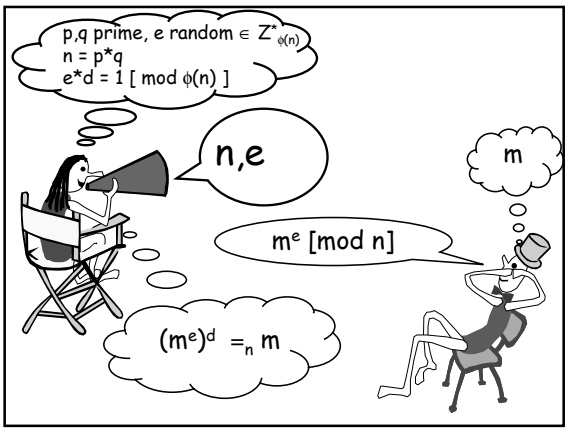
Theorem.
$d*e = 1 \bmod (p-1)(q-1)$
Example.
$m^{145} = m \pmod{65}$
Modulo 5:
$m^{145} = m^{4*36+1} = m \pmod 5$
Modulo 13:
$m^{145} = m^{12*12+1} = m \pmod{13}$

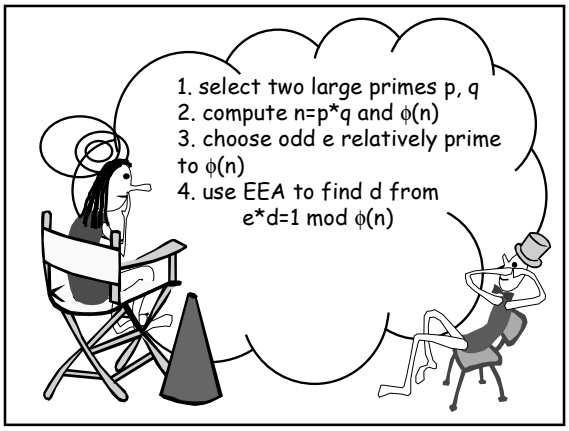
Exponential Inverses

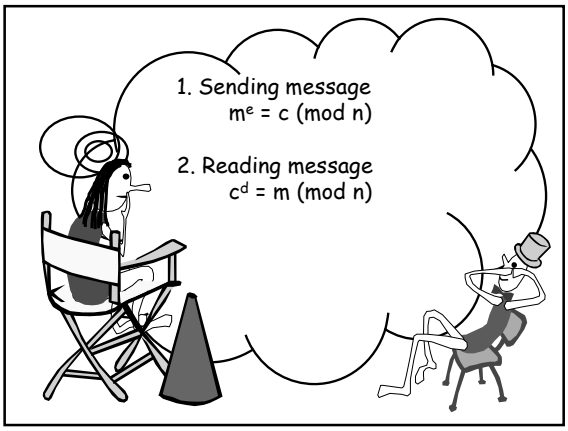
Theorem.
$d*e = 1 \bmod (p-1)(q-1)$
Proof.
$m^{d*e} = m^{1 + k(p-1)(q-1)} \pmod n$
The system of congruences:
$m^{d*e} = m \pmod p$
$m^{d*e} = m \pmod q$

Chinese Remainder Theorem

Theorem.
GCD(p, q) = 1
$x = a \pmod p$
$x = b \pmod q$
The system has a unique solution mod (p*q)







RSA example

1. p = 61, q = 53
2. n = 3233, φ(n) = 60*52 = 3120
3. e = 37 (there are many to choose from)
4. EEA: 1 = (-3)*3120+253*37
   d = 253

Public key (3233, 37)
Private key 253

RSA example

Public key (3233, 37)
Private key 253

Send: $c = m^{37} \bmod 3233$

Read: $m = c^{253} \bmod 3233$

Authentication

How Alice can be sure that that the message came from Bob?

Authentication

How Alice can be sure that that the message came from Bob?

Bob can encode his signature using d

$S^d \pmod n$

Alice will read the signature using e

$S^{d*e} = S \pmod n$

Cracking RSA

In 1977 Rivest, Shamir and Adleman published 129 key number (452 bits)

and promised $100 to the first person who factor it

Cracking RSA

Team from Bellcore and MIT solved (in 1993-1994) this by using 1600 computers (over the internet) within 8 months.

THE MAGIC WORDS ARE
SQUEAMISH OSSIFRAGE

Cracking RSA

The current record:

RSA-674: Nov., 2005

Study Bee

- Fast Exponentiation
- EEA
- Modular inverses
- FLT
- CRT