Class 9

RSA

Invented by Ronal Riverst, Adi Shamir, Leonard Alleman (1978)

Based on a trapdoor one-way function, such the one used in Diffie-Hellman key generation algorithm

RSA (1)

In general:

1. Choose two large primes, *p* and *q*
2. Compute
   $n = p \times q$ *and* $z = (p - 1) \times (q - 1)$.
3. Choose number relatively prime to *z*
   call it *d.*
4. Find *e* such that $e \times d = 1 \bmod z$.

P (plaintext), falls in the interval $0 \leq P < n$.

Plaintext is group into blocks of *k* bits, where *k* is the largest integer for which $2^k < n$ is true.

To encrypt a message, P, compute $C = P^e \pmod n$. To decrypt C, compute $P = C^d \pmod n$
The public key consists of the pair (e, n), and the private key consists of (d, n).

RSA (2)

Plaintext (P)			Ciphertext (C)		After decryption	
Symbolic	Numeric	P^3	P^3 (mod 33)	C^7	C^7 (mod 33)	Symbolic
S	19	6859	28	13492928512	19	S
U	21	9261	21	1801088541	21	U
Z	26	17576	20	1280000000	26	Z
A	01	1	1	1	01	A
N	14	2744	5	78125	14	N
N	14	2744	5	78125	14	N
E	05	125	26	8031810176	05	E

Sender's computation

Receiver's computation

An example of the RSA algorithm

Using the RSA public key crypto-system with a=1, b=2 …. Y=25, z=26.

(a) If p=5 and q=13. List five legal values for d.

How about 5, 7, 11, 13, and 17.

(b) If p=5, q=31, and d=37, find *e.*

If z=120=(5-1)(31-1)

Then,
37. *e=1mod(120)*
121, 241, 361, 481….

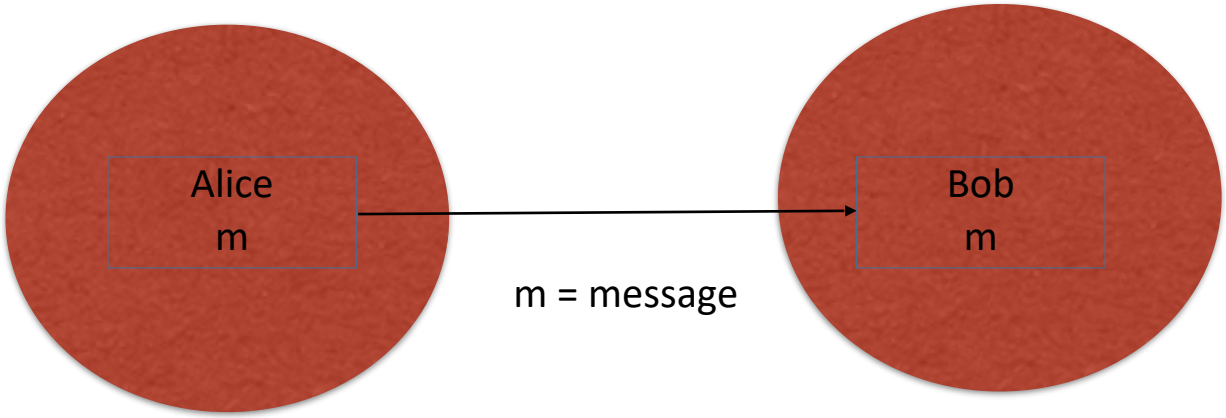
For 481/37 = 13=*e*

(c) Using p=3 , q=11, and d=9, find e and encrypt “hello”

Implementation of Cryptographic protocols

Cryptographic protocols consist on an exchange between participants

Roles



A single entity can take any of the roles, how about Eve?

Trust

The basis people use to DEAL. Incentive to behave well.

Different sources of trust:

- Ethics
- Reputation
- Law
- Physical Threat
- Mutually Assured Destruction (MAD)

Risk

In cryptographic protocols is used to express a level of TRUST.

Sometimes managed by risk-management techniques.

Incentive

Real motivation/intention behind creation of the cryptographic protocol

Trust in Cryptographic Protocols

The goal of Cryptographic Protocols is to minimize the amount of trust required.

Paranoia model as a tool for designing cryptographic protocols.

Documented trust requirements would list the risks.

Messages and Steps

Modularization

Functionality can be split into several protocol layers

The transport layer

For cryptographers, the transport layer is the underlying communication system that permits parties to communicate

Protocol and Message Identity

Provides protocol and message identifiers

Which protocol belongs to and which message within that protocol is.

Two parts

Version information | cryptographic protocol the message belongs to

Message encoding and parsing

Data elements of the message transformed into a sequence

of bytes

Encoding is use for variable size data

Protocol Execution States

The states contains all the information to complete the protocol

Errors

Checks to verify the:

protocol type

message type

protocol execution state

Avoid error retransmission, local handling.