ASYMMETRIC ENCRYPTION

Recommended Book

Steven Levy. *Crypto*. Penguin books. 2001.

A non-technical account of the history of public-key cryptography and the colorful characters involved.

Recall Symmetric Cryptography

- Before Alice and Bob can communicate securely, they need to have a common secret key K_{AB}.
- If Alice wishes to also communicate with Charlie then she and Charlie must also have another common secret key K_{AC}.
- If Alice generates K_{AB}, K_{AC}, they must be communicated to her partners over private and authenticated channels.

Public Key Encryption

- Alice has a secret key that is shared with nobody, and an associated public key that is known to everybody.
- Anyone (Bob, Charlie, . . .) can use Alice's public key to send her an encrypted message which only she can decrypt.

Think of the public key like a phone number that you can look up in a database

Public Key Encryption

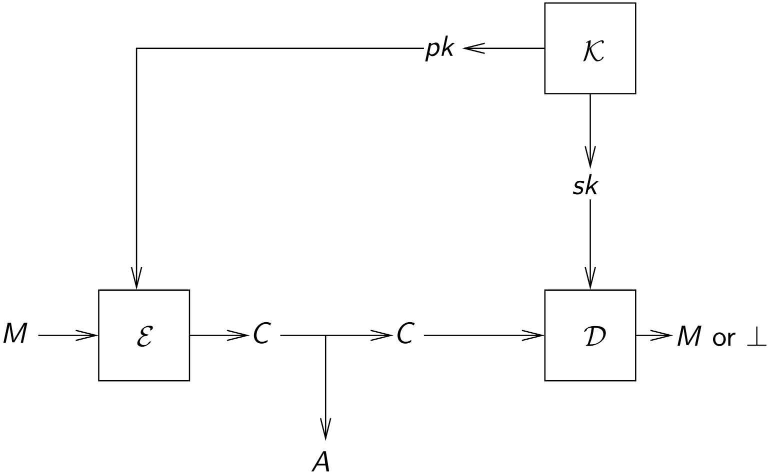
- Alice has a secret key that is shared with nobody, and an associated public key that is known to everybody.
- Anyone (Bob, Charlie, . . .) can use Alice's public key to send her an encrypted message which only she can decrypt.

Think of the public key like a phone number that you can look up in a database

- Senders don't need secrets
- There are no shared secrets

Syntax of PKE

A public-key (or asymmetric) encryption scheme $\mathcal{AE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ consists of three algorithms, where



How it Works

Step 1: Key generation
Alice locally computers $(pk, sk) \xleftarrow{\$} \mathcal{K}$ and stores sk.

Step 2: Alice enables any prospective sender to get pk.

Step 3: The sender encrypts under pk and Alice decrypts under sk.

We don't require privacy of pk but we do require authenticity: the sender should be assured pk is really Alice's key and not someone else's. One could

- Put public keys in a trusted but public "phone book", say a cryptographic DNS.
- Use certificates as we will see later.

Security of PKE Schemes: Issues

The issues are the same as for symmetric encryption:

- Want general purpose schemes
- Security should not rely on assumptions about usage setting
- Want to prevent leakage of partial information about plaintexts

Security requirements

Suppose sender computes

$$C_1 \xleftarrow{\$} \mathcal{E}_{pk}(M_1)\,;\ \cdots\ ;\ C_q \xleftarrow{\$} \mathcal{E}_{pk}(M_q)$$

Adversary A has $C_1, \ldots, C_q$

What if A	
Retrieves sk	Bad!
Retrieves M_1	Bad!

But also ...

Security requirements

We want to hide all partial information about the data stream.

Examples of partial information:

- Does $M_1 = M_2$?
- What is first bit of M_1?
- What is XOR of first bits of M_1, M_2?

Security requirements

We want to hide all partial information about the data stream.

Examples of partial information:

- Does $M_1 = M_2$?
- What is first bit of M_1?
- What is XOR of first bits of M_1, M_2?

Something we won't hide: the length of the message

New Issue

The adversary needs to be given the public key.

Intuition for definition of IND

Consider encrypting one of two possible message streams, either

$$M_0^1, \ldots, M_0^q$$

or

$$M_1^1, \ldots, M_1^q$$

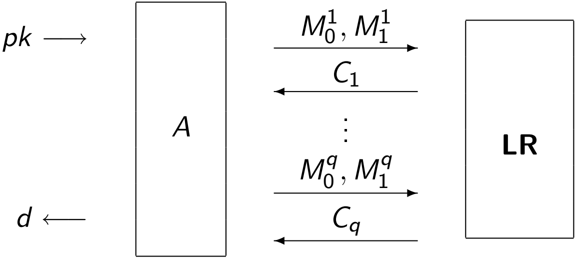
Adversary, given ciphertexts and both data streams, has to figure out which of the two streams was encrypted.

ind-cpa-adversaries

Let $\mathcal{AE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an public-key encryption scheme

An ind-cpa adversary A has input pk and an oracle **LR**

- It can make a query M_0, M_1 consisting of any two equal-length messages
- It can do this many times
- Each time it gets back a ciphertext
- It eventually outputs a bit



$pk \longrightarrow$

A

M_0^1, M_1^1

C_1

$\vdots$

M_0^q, M_1^q

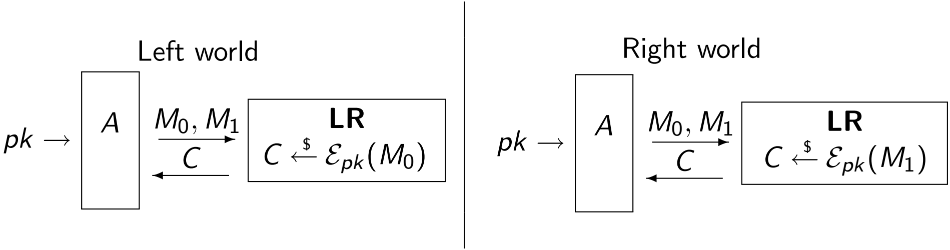
C_q

LR

$d \longleftarrow$

ind-cpa-adversaries

Let $\mathcal{AE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a public-key encryption scheme



Left world

$pk \rightarrow$ A

M_0, M_1

C

LR

$C \xleftarrow{\$} \mathcal{E}_{pk}(M_0)$

Right world

$pk \rightarrow$ A

M_0, M_1

C

LR

$C \xleftarrow{\$} \mathcal{E}_{pk}(M_1)$

A's output d	Intended meaning: I think I am in the
1	Right world
0	Left world

The harder it is for A to guess world it is in, the more "secure" $\mathcal{AE}$ is as an encryption scheme.

The games

Let $\mathcal{AE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a public-key encryption scheme

```
Game $\mathrm{Left}_{\mathcal{AE}}$
procedure Initialize
$(pk, sk) \xleftarrow{\$} \mathcal{K}$ ; return $pk$
procedure LR$(M_0, M_1)$
Return $C \xleftarrow{\$} \mathcal{E}_{pk}(M_0)$
```

```
Game $\mathrm{Right}_{\mathcal{AE}}$
procedure Initialize
$(pk, sk) \xleftarrow{\$} \mathcal{K}$ ; return $pk$
procedure LR$(M_0, M_1)$
Return $C \xleftarrow{\$} \mathcal{E}_{pk}(M_1)$
```

Associated to $\mathcal{AE}, A$ are the probabilities

$$\Pr\left[\mathrm{Left}^{A}_{\mathcal{AE}} \Rightarrow 1\right] \qquad \Big| \qquad \Pr\left[\mathrm{Right}^{A}_{\mathcal{AE}} \Rightarrow 1\right]$$

that A outputs 1 in each world. The ind-cpa advantage of A is

$$\mathbf{Adv}^{\mathrm{ind\text{-}cpa}}_{\mathcal{AE}}(A) = \Pr\left[\mathrm{Right}^{A}_{\mathcal{AE}} \Rightarrow 1\right] - \Pr\left[\mathrm{Left}^{A}_{\mathcal{AE}} \Rightarrow 1\right]$$

Simplification

We may assume A makes only one **LR** query. It can be shown that this can decrease its advantage by at most the number of **LR** queries.

Building a PKE Scheme

We would like security to result from the hardness of computing discrete logarithms.

Let the receiver's public key be g where $G = \langle g \rangle$ is a cyclic group. Let's let the encryption of x be g^x. Then

$$\underbrace{g^x}_{\mathcal{E}_g(x)} \xrightarrow{\text{hard}} x$$

so to recover x, adversary must compute discrete logarithms, and we know it can't, so are we done?

Building a PKE Scheme

We would like security to result from the hardness of computing discrete logarithms.

Let the receiver's public key be g where $G = \langle g \rangle$ is a cyclic group. Let's let the encryption of x be g^x. Then

$$\underbrace{g^x}_{\mathcal{E}_g(x)} \xrightarrow{\text{hard}} x$$

so to recover x, adversary must compute discrete logarithms, and we know it can't, so are we done?

Problem: Legitimate receiver needs to compute discrete logarithm to decrypt too! But decryption needs to be feasible.

Building a PKE Scheme

We would like security to result from the hardness of computing discrete logarithms.

Let the receiver's public key be g where $G = \langle g \rangle$ is a cyclic group. Let's let the encryption of x be g^x. Then

$$\underbrace{g^x}_{\mathcal{E}_g(x)} \xrightarrow{\text{hard}} x$$

so to recover x, adversary must compute discrete logarithms, and we know it can't, so are we done?

Problem: Legitimate receiver needs to compute discrete logarithm to decrypt too! But decryption needs to be feasible.

Above, receiver has no secret key!

DH Key Exchange

Let $G = \langle g \rangle$ be a cyclic group of order m.

$$\begin{array}{ccc} \text{Alice} & & \text{Bob} \\ x \xleftarrow{\$} \mathbf{Z}_m;\, X \leftarrow g^x & \begin{array}{c} \xrightarrow{\quad \text{X} \quad} \\ \xleftarrow{\quad \text{Y} \quad} \end{array} & y \xleftarrow{\$} \mathbf{Z}_m;\, Y \leftarrow g^y \end{array}$$

Then

$$Y^x = (g^y)^x = g^{xy} = (g^x)^y = X^y$$

- Alice can compute $K = Y^x$
- Bob can compute $K = X^y$
- But adversary wanting to compute K is faced with

$$g^x, g^y \longrightarrow g^{xy}$$

which is exactly the CDH problem and is computationally hard.

So this enables Alice and Bob to get a common shared key which they can then use to secure their communications.

The El Gamal Scheme: Idea

We can turn DH key exchange into a public key encryption scheme via

- Let Alice have public key g^x and secret key x
- If Bob wants to encrypt M for Alice, he
    - Picks y and sends g^y to Alice
    - Encrypts M under $g^{xy} = (g^x)^y$ and sends ciphertext to Alice.
- But Alice can recompute $g^{xy} = (g^y)^x$ because
    - g^y is in the received ciphertext
    - x is her secret key

Thus she can decrypt and adversary is still faced with CDH .

EG Encryption, in Full

Let $G = \langle g \rangle$ be a cyclic group of order m. The EG PKE scheme $\mathcal{AE}_{\mathrm{EG}} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is defined by

```
**Alg** $\mathcal{K}$
$x \xleftarrow{\$} \mathbf{Z}_m$
$X \leftarrow g^x$
return $(X, x)$
```

```
**Alg** $\mathcal{E}_X(M)$
$y \xleftarrow{\$} \mathbf{Z}_m$; $Y \leftarrow g^y$
$K \leftarrow X^y$
$W \leftarrow K \cdot M$
return $(Y, W)$
```

```
**Alg** $\mathcal{D}_x(Y, W)$
$K = Y^x$
$M \leftarrow W \cdot K^{-1}$
return $M$
```

We assume the message $M \in G$ is a group element.

Correct decryption is assured because

$$K = X^y = g^{xy} = Y^x$$

Implementation uses several algorithms we have studied before: exponentiation, inverse.

Security of $\mathcal{AE}_{\mathrm{EG}}$

secret key $= x \in \mathbf{Z}_m$, where $m = |G|$
public key $= X = g^x \in G = \langle g \rangle$

```
algorithm $\mathcal{E}_X(M)$
$y \xleftarrow{\$} \mathbf{Z}_m$;  $Y \leftarrow g^y$
$K \leftarrow X^y$;  $W \leftarrow K \cdot M$
return  $(Y, W)$
```

```
algorithm $\mathcal{D}_x(Y, W)$
$K \leftarrow Y^x$;  $M \leftarrow W \cdot K^{-1}$
return  $M$
```

- To find x given X, adversary must solve DL problem

Security of $\mathcal{AE}_{\mathrm{EG}}$

secret key $= x \in \mathbf{Z}_m$, where $m = |G|$
public key $= X = g^x \in G = \langle g \rangle$

```
algorithm $\mathcal{E}_X(M)$
$y \xleftarrow{\$} \mathbf{Z}_m$;  $Y \leftarrow g^y$
$K \leftarrow X^y$;  $W \leftarrow K \cdot M$
return  $(Y, W)$
```

```
algorithm $\mathcal{D}_x(Y, W)$
$K \leftarrow Y^x$;  $M \leftarrow W \cdot K^{-1}$
return  $M$
```

- To find x given X, adversary must solve DL problem
- To find M given $X, (Y, W)$, adversary must compute $K = g^{xy}$, meaning solve CDH problem

Security of $\mathcal{AE}_{\mathrm{EG}}$

secret key $= x \in \mathbf{Z}_m$, where $m = |G|$
public key $= X = g^x \in G = \langle g \rangle$

```
algorithm $\mathcal{E}_X(M)$
    $y \xleftarrow{\$} \mathbf{Z}_m$; $Y \leftarrow g^y$
    $K \leftarrow X^y$; $W \leftarrow K \cdot M$
    return $(Y, W)$
```

```
algorithm $\mathcal{D}_x(Y, W)$
    $K \leftarrow Y^x$; $M \leftarrow W \cdot K^{-1}$
    return $M$
```

- To find x given X, adversary must solve DL problem
- To find M given $X, (Y, W)$, adversary must compute $K = g^{xy}$, meaning solve CDH problem
- But what prevents leakage of partial information about M? Is the scheme IND-CPA secure?

Security of $\mathcal{AE}_{\mathrm{EG}}$ in $\mathbf{Z}_p^*$

In $G = \mathbf{Z}_p^*$, where p is a prime

- DL, CDH are hard, yet
- There is an attack showing $\mathcal{AE}_{\mathrm{EG}}$ is NOT IND-CPA secure

Number theory

Number theory is fun!

Squares

We say that a is a square (or quadratic residue) modulo p if there exists b such that $b^2 \equiv a \pmod{p}$.

We let

$$J_p(a) = \begin{cases} 1 & \text{if } a \text{ is a square mod } p \\ 0 & \text{if } a \bmod p = 0 \\ -1 & \text{otherwise} \end{cases}$$

be the Legendre or Jacobi symbol of a modulo p.

Let $p = 11$. Then

- Is 4 a square modulo p?

Squares

We say that a is a square (or quadratic residue) modulo p if there exists b such that $b^2 \equiv a \pmod{p}$.

We let

$$J_p(a) \;=\; \begin{cases} 1 & \text{if } a \text{ is a square mod } p \\ 0 & \text{if } a \bmod p = 0 \\ -1 & \text{otherwise} \end{cases}$$

be the Legendre or Jacobi symbol of a modulo p.

Let $p = 11$. Then

- Is 4 a square modulo p?
  YES because $2^2 \equiv 4 \pmod{11}$
- Is 5 a square modulo p?

Squares

We say that a is a square (or quadratic residue) modulo p if there exists b such that $b^2 \equiv a \pmod{p}$.

We let

$$J_p(a) = \begin{cases} 1 & \text{if } a \text{ is a square mod } p \\ 0 & \text{if } a \bmod p = 0 \\ -1 & \text{otherwise} \end{cases}$$

be the Legendre or Jacobi symbol of a modulo p.

Let $p = 11$. Then

- Is 4 a square modulo p?
  YES because $2^2 \equiv 4 \pmod{11}$
- Is 5 a square modulo p?
  YES because $4^2 \equiv 5 \pmod{11}$
- What is $J_{11}(5)$?

Squares

We say that a is a square (or quadratic residue) modulo p if there exists b such that $b^2 \equiv a \pmod{p}$.

We let

$$J_p(a) = \begin{cases} 1 & \text{if } a \text{ is a square mod } p \\ 0 & \text{if } a \bmod p = 0 \\ -1 & \text{otherwise} \end{cases}$$

be the Legendre or Jacobi symbol of a modulo p.

Let $p = 11$. Then

- Is 4 a square modulo p?
  YES because $2^2 \equiv 4 \pmod{11}$
- Is 5 a square modulo p?
  YES because $4^2 \equiv 5 \pmod{11}$
- What is $J_{11}(5)$?
  It equals $+1$

The set of squares

We let

$$\begin{aligned} \mathrm{QR}(\mathbf{Z}_p^*) &= \{a \in \mathbf{Z}_p^* \ : \ a \text{ is a square mod } p\} \\ &= \{a \in \mathbf{Z}_p^* \ : \ \exists b \in \mathbf{Z}_p^* \text{ such that } b^2 \equiv a \pmod{p}\} \end{aligned}$$

Example

Let $p = 11$

a	1	2	3	4	5	6	7	8	9	10
$a^2 \bmod 11$										

Example

Let $p = 11$

a	1	2	3	4	5	6	7	8	9	10
$a^2 \bmod 11$	1									

Example

Let $p = 11$

a	1	2	3	4	5	6	7	8	9	10
$a^2 \bmod 11$	1	4								

Example

Let $p = 11$

a	1	2	3	4	5	6	7	8	9	10
$a^2 \bmod 11$	1	4	9							

Example

Let $p = 11$

a	1	2	3	4	5	6	7	8	9	10
$a^2 \bmod 11$	1	4	9	5						

Example

Let $p = 11$

a	1	2	3	4	5	6	7	8	9	10
$a^2 \bmod 11$	1	4	9	5	3					

Example

Let $p = 11$

a	1	2	3	4	5	6	7	8	9	10
$a^2 \bmod 11$	1	4	9	5	3	3				

Example

Let $p = 11$

a	1	2	3	4	5	6	7	8	9	10
$a^2 \bmod 11$	1	4	9	5	3	3	5			

Example

Let $p = 11$

a	1	2	3	4	5	6	7	8	9	10
$a^2 \bmod 11$	1	4	9	5	3	3	5	9		

Example

Let $p = 11$

a	1	2	3	4	5	6	7	8	9	10
$a^2 \bmod 11$	1	4	9	5	3	3	5	9	4	

Example

Let $p = 11$

a	1	2	3	4	5	6	7	8	9	10
$a^2 \bmod 11$	1	4	9	5	3	3	5	9	4	1

Then

$$\mathrm{QR}(\mathbf{Z}_p^*) = \{1, 3, 4, 5, 9\}$$

a	1	2	3	4	5	6	7	8	9	10
$J_{11}(a)$	1	-1	1	1	1	-1	-1	-1	1	-1

Observe

- There are 5 squares and 5 non-squares.
- Every square has exactly 2 square roots.

Relation to discrete log

Recall that 2 is a generator of $\mathbf{Z}_{11}^*$

a	1	2	3	4	5	6	7	8	9	10
$\mathrm{DLog}_{\mathbf{Z}_{11}^*,2}(a)$	0	1	8	2	4	9	7	3	6	5
$J_{11}(a)$	1	-1	1	1	1	-1	-1	-1	1	-1

Relation to discrete log

Recall that 2 is a generator of $\mathbf{Z}_{11}^*$

a	1	2	3	4	5	6	7	8	9	10
$\mathrm{DLog}_{\mathbf{Z}_{11}^*,2}(a)$	0	1	8	2	4	9	7	3	6	5
$J_{11}(a)$	1	-1	1	1	1	-1	-1	-1	1	-1

so

$$J_{11}(a) = 1 \quad \text{iff} \quad \mathrm{DLog}_{\mathbf{Z}_{11}^*,2}(a) \text{ is even}$$

This makes sense because for any generator g,

$$g^{2j} = (g^j)^2$$

is always a square!

Squares and discrete logs

Fact: If $p \geq 3$ is a prime and g is a generator of $\mathbf{Z}_p^*$ then

$$\mathrm{QR}(\mathbf{Z}_p^*) = \{g^i \ : \ 0 \leq i \leq p-2 \text{ and } i \text{ is even}\}$$

Example: If $p = 11$ and $g = 2$ then $p - 2 = 9$ and the squares are

- $2^0 \bmod 11 = 1$
- $2^2 \bmod 11 = 4$
- $2^4 \bmod 11 = 5$
- $2^6 \bmod 11 = 9$
- $2^8 \bmod 11 = 3$

Computing the Legendre symbol

Is there an algorithm that given p and $a \in \mathbf{Z}_p^*$ returns $J_p(a)$, meaning determines whether or not a is a square mod p?

Computing the Legendre symbol

Is there an algorithm that given p and $a \in \mathbf{Z}_p^*$ returns $J_p(a)$, meaning determines whether or not a is a square mod p?

Sure!

```
**Alg** $\text{TEST-SQ}(p, a)$
Let $g$ be a generator of $\mathbf{Z}_p^*$
Let $i \leftarrow \text{DLog}_{\mathbf{Z}_p^*, g}(a)$
if $i$ is even then return 1 else return $-1$
```

Computing the Legendre symbol

Is there an algorithm that given p and $a \in \mathbf{Z}_p^*$ returns $J_p(a)$, meaning determines whether or not a is a square mod p?

Sure!

```
**Alg** TEST-SQ$(p, a)$
Let $g$ be a generator of $\mathbf{Z}_p^*$
Let $i \leftarrow \mathrm{DLog}_{\mathbf{Z}_p^*,g}(a)$
if $i$ is even then return 1 else return $-1$
```

This is correct, but

- How do we find g?
- How do we compute $\mathrm{DLog}_{\mathbf{Z}_p^*,g}(a)$?

Fermat's Theorem

Fact: If $p \geq 3$ is a prime then for any a

$$J_p(a) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Example: Let $p = 11$.

- Let $a = 5$. We know that 5 is a square, meaning $J_{11}(5) = 1$. Now compute

$$a^{\frac{p-1}{2}} \equiv 5^5 \equiv (25)(25)(5) \equiv 3 \cdot 3 \cdot 5 \equiv 45 \equiv 1 \pmod{11}.$$

- Let $a = 6$. We know that 6 is not a square, meaning $J_{11}(6) = -1$. Now compute

$$a^{\frac{p-1}{2}} \equiv 6^5 \equiv (36)(36)(6) \equiv 3 \cdot 3 \cdot 6 \equiv 54 \equiv -1 \pmod{11}.$$

Fermat's Theorem

Fact: If $p \geq 3$ is a prime then for any a

$$J_p(a) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

This yields a cubic-time algorithm to compute the Legendre symbol, meaning determine whether or not a given number is a square:

```
**Alg** TEST-SQ$(p, a)$
$s \leftarrow a^{\frac{p-1}{2}} \bmod p$
if $s = 1$ then return 1 else return $-1$
```

Multiplicity of Legendre symbol

Fact: If $p \geq 3$ is a prime then for any a, b

$$J_p(ab) = J_p(a) \cdot J_p(b)$$

Example: Let $p = 11$.

a	1	2	3	4	5	6	7	8	9	10
$J_{11}(a)$	1	-1	1	1	1	-1	-1	-1	1	-1

a	b	ab	$J_{11}(a)$	$J_{11}(b)$	$J_{11}(ab)$	$J_{11}(a) \cdot J_{11}(b)$

Multiplicity of Legendre symbol

Fact: If $p \geq 3$ is a prime then for any a, b

$$J_p(ab) = J_p(a) \cdot J_p(b)$$

Example: Let $p = 11$.

a	1	2	3	4	5	6	7	8	9	10
$J_{11}(a)$	1	-1	1	1	1	-1	-1	-1	1	-1

a	b	ab	$J_{11}(a)$	$J_{11}(b)$	$J_{11}(ab)$	$J_{11}(a) \cdot J_{11}(b)$
5						

Multiplicity of Legendre symbol

Fact: If $p \geq 3$ is a prime then for any a, b

$$J_p(ab) = J_p(a) \cdot J_p(b)$$

Example: Let $p = 11$.

a	1	2	3	4	5	6	7	8	9	10
$J_{11}(a)$	1	-1	1	1	1	-1	-1	-1	1	-1

a	b	ab	$J_{11}(a)$	$J_{11}(b)$	$J_{11}(ab)$	$J_{11}(a) \cdot J_{11}(b)$
5	6					

Multiplicity of Legendre symbol

Fact: If $p \geq 3$ is a prime then for any a, b

$$J_p(ab) = J_p(a) \cdot J_p(b)$$

Example: Let $p = 11$.

a	1	2	3	4	5	6	7	8	9	10
$J_{11}(a)$	1	-1	1	1	1	-1	-1	-1	1	-1

a	b	ab	$J_{11}(a)$	$J_{11}(b)$	$J_{11}(ab)$	$J_{11}(a) \cdot J_{11}(b)$
5	6	8				

Multiplicity of Legendre symbol

Fact: If $p \geq 3$ is a prime then for any a, b

$$J_p(ab) = J_p(a) \cdot J_p(b)$$

Example: Let $p = 11$.

a	1	2	3	4	5	6	7	8	9	10
$J_{11}(a)$	1	-1	1	1	1	-1	-1	-1	1	-1

a	b	ab	$J_{11}(a)$	$J_{11}(b)$	$J_{11}(ab)$	$J_{11}(a) \cdot J_{11}(b)$
5	6	8	1			

Multiplicity of Legendre symbol

Fact: If $p \geq 3$ is a prime then for any a, b

$$J_p(ab) = J_p(a) \cdot J_p(b)$$

Example: Let $p = 11$.

a	1	2	3	4	5	6	7	8	9	10
$J_{11}(a)$	1	-1	1	1	1	-1	-1	-1	1	-1

a	b	ab	$J_{11}(a)$	$J_{11}(b)$	$J_{11}(ab)$	$J_{11}(a) \cdot J_{11}(b)$
5	6	8	1	-1		

Multiplicity of Legendre symbol

Fact: If $p \geq 3$ is a prime then for any a, b

$$J_p(ab) = J_p(a) \cdot J_p(b)$$

Example: Let $p = 11$.

a	1	2	3	4	5	6	7	8	9	10
$J_{11}(a)$	1	-1	1	1	1	-1	-1	-1	1	-1

a	b	ab	$J_{11}(a)$	$J_{11}(b)$	$J_{11}(ab)$	$J_{11}(a) \cdot J_{11}(b)$
5	6	8	1	-1	-1	

Multiplicity of Legendre symbol

Fact: If $p \geq 3$ is a prime then for any a, b

$$J_p(ab) = J_p(a) \cdot J_p(b)$$

Example: Let $p = 11$.

a	1	2	3	4	5	6	7	8	9	10
$J_{11}(a)$	1	-1	1	1	1	-1	-1	-1	1	-1

a	b	ab	$J_{11}(a)$	$J_{11}(b)$	$J_{11}(ab)$	$J_{11}(a) \cdot J_{11}(b)$
5	6	8	1	-1	-1	-1

Multiplicity of Legendre symbol

Fact: If $p \geq 3$ is a prime then for any a, b

$$J_p(ab) = J_p(a) \cdot J_p(b)$$

Example: Let $p = 11$.

a	1	2	3	4	5	6	7	8	9	10
$J_{11}(a)$	1	-1	1	1	1	-1	-1	-1	1	-1

a	b	ab	$J_{11}(a)$	$J_{11}(b)$	$J_{11}(ab)$	$J_{11}(a) \cdot J_{11}(b)$
5	6	8	1	-1	-1	-1
2						

Multiplicity of Legendre symbol

Fact: If $p \geq 3$ is a prime then for any a, b

$$J_p(ab) = J_p(a) \cdot J_p(b)$$

Example: Let $p = 11$.

a	1	2	3	4	5	6	7	8	9	10
$J_{11}(a)$	1	-1	1	1	1	-1	-1	-1	1	-1

a	b	ab	$J_{11}(a)$	$J_{11}(b)$	$J_{11}(ab)$	$J_{11}(a) \cdot J_{11}(b)$
5	6	8	1	-1	-1	-1
2	7					

Multiplicity of Legendre symbol

Fact: If $p \geq 3$ is a prime then for any a, b

$$J_p(ab) = J_p(a) \cdot J_p(b)$$

Example: Let $p = 11$.

a	1	2	3	4	5	6	7	8	9	10
$J_{11}(a)$	1	-1	1	1	1	-1	-1	-1	1	-1

a	b	ab	$J_{11}(a)$	$J_{11}(b)$	$J_{11}(ab)$	$J_{11}(a) \cdot J_{11}(b)$
5	6	8	1	-1	-1	-1
2	7	3				

Multiplicity of Legendre symbol

Fact: If $p \geq 3$ is a prime then for any a, b

$$J_p(ab) = J_p(a) \cdot J_p(b)$$

Example: Let $p = 11$.

a	1	2	3	4	5	6	7	8	9	10
$J_{11}(a)$	1	-1	1	1	1	-1	-1	-1	1	-1

a	b	ab	$J_{11}(a)$	$J_{11}(b)$	$J_{11}(ab)$	$J_{11}(a) \cdot J_{11}(b)$
5	6	8	1	-1	-1	-1
2	7	3	-1			

Multiplicity of Legendre symbol

Fact: If $p \geq 3$ is a prime then for any a, b

$$J_p(ab) = J_p(a) \cdot J_p(b)$$

Example: Let $p = 11$.

a	1	2	3	4	5	6	7	8	9	10
$J_{11}(a)$	1	-1	1	1	1	-1	-1	-1	1	-1

a	b	ab	$J_{11}(a)$	$J_{11}(b)$	$J_{11}(ab)$	$J_{11}(a) \cdot J_{11}(b)$
5	6	8	1	-1	-1	-1
2	7	3	-1	-1		

Multiplicity of Legendre symbol

Fact: If $p \geq 3$ is a prime then for any a, b

$$J_p(ab) = J_p(a) \cdot J_p(b)$$

Example: Let $p = 11$.

a	1	2	3	4	5	6	7	8	9	10
$J_{11}(a)$	1	-1	1	1	1	-1	-1	-1	1	-1

a	b	ab	$J_{11}(a)$	$J_{11}(b)$	$J_{11}(ab)$	$J_{11}(a) \cdot J_{11}(b)$
5	6	8	1	-1	-1	-1
2	7	3	-1	-1	1	

Multiplicity of Legendre symbol

Fact: If $p \geq 3$ is a prime then for any a, b

$$J_p(ab) = J_p(a) \cdot J_p(b)$$

Example: Let $p = 11$.

a	1	2	3	4	5	6	7	8	9	10
$J_{11}(a)$	1	-1	1	1	1	-1	-1	-1	1	-1

a	b	ab	$J_{11}(a)$	$J_{11}(b)$	$J_{11}(ab)$	$J_{11}(a) \cdot J_{11}(b)$
5	6	8	1	-1	-1	-1
2	7	3	-1	-1	1	1

Inversion of Legendre symbol

Fact: If $p \geq 3$ is a prime then for any $a \in \mathbf{Z}_p^*$

$$J_p(a^{-1}) = J_p(a)$$

Example: $p = 11$

a	1	2	3	4	5	6	7	8	9	10
$J_{11}(a)$	1	-1	1	1	1	-1	-1	-1	1	-1

a	a^{-1}	$J_{11}(a)$	$J_{11}(a^{-1})$

Inversion of Legendre symbol

Fact: If $p \geq 3$ is a prime then for any $a \in \mathbf{Z}_p^*$

$$J_p(a^{-1}) = J_p(a)$$

Example: $p = 11$

a	1	2	3	4	5	6	7	8	9	10
$J_{11}(a)$	1	-1	1	1	1	-1	-1	-1	1	-1

a	a^{-1}	$J_{11}(a)$	$J_{11}(a^{-1})$
3			

Inversion of Legendre symbol

Fact: If $p \geq 3$ is a prime then for any $a \in \mathbf{Z}_p^*$

$$J_p(a^{-1}) = J_p(a)$$

Example: $p = 11$

a	1	2	3	4	5	6	7	8	9	10
$J_{11}(a)$	1	-1	1	1	1	-1	-1	-1	1	-1

a	a^{-1}	$J_{11}(a)$	$J_{11}(a^{-1})$
3	4		

Inversion of Legendre symbol

Fact: If $p \geq 3$ is a prime then for any $a \in \mathbf{Z}_p^*$

$$J_p(a^{-1}) = J_p(a)$$

Example: $p = 11$

a	1	2	3	4	5	6	7	8	9	10
$J_{11}(a)$	1	-1	1	1	1	-1	-1	-1	1	-1

a	a^{-1}	$J_{11}(a)$	$J_{11}(a^{-1})$
3	4	1	

Inversion of Legendre symbol

Fact: If $p \geq 3$ is a prime then for any $a \in \mathbf{Z}_p^*$

$$J_p(a^{-1}) = J_p(a)$$

Example: $p = 11$

a	1	2	3	4	5	6	7	8	9	10
$J_{11}(a)$	1	-1	1	1	1	-1	-1	-1	1	-1

a	a^{-1}	$J_{11}(a)$	$J_{11}(a^{-1})$
3	4	1	1

Inversion of Legendre symbol

Fact: If $p \geq 3$ is a prime then for any $a \in \mathbf{Z}_p^*$

$$J_p(a^{-1}) = J_p(a)$$

Example: $p = 11$

a	1	2	3	4	5	6	7	8	9	10
$J_{11}(a)$	1	-1	1	1	1	-1	-1	-1	1	-1

a	a^{-1}	$J_{11}(a)$	$J_{11}(a^{-1})$
3	4	1	1
7			

Inversion of Legendre symbol

Fact: If $p \geq 3$ is a prime then for any $a \in \mathbf{Z}_p^*$

$$J_p(a^{-1}) = J_p(a)$$

Example: $p = 11$

a	1	2	3	4	5	6	7	8	9	10
$J_{11}(a)$	1	-1	1	1	1	-1	-1	-1	1	-1

a	a^{-1}	$J_{11}(a)$	$J_{11}(a^{-1})$
3	4	1	1
7	8		

Inversion of Legendre symbol

Fact: If $p \geq 3$ is a prime then for any $a \in \mathbf{Z}_p^*$

$$J_p(a^{-1}) = J_p(a)$$

Example: $p = 11$

a	1	2	3	4	5	6	7	8	9	10
$J_{11}(a)$	1	-1	1	1	1	-1	-1	-1	1	-1

a	a^{-1}	$J_{11}(a)$	$J_{11}(a^{-1})$
3	4	1	1
7	8	-1	

Inversion of Legendre symbol

Fact: If $p \geq 3$ is a prime then for any $a \in \mathbf{Z}_p^*$

$$J_p(a^{-1}) = J_p(a)$$

Example: $p = 11$

a	1	2	3	4	5	6	7	8	9	10
$J_{11}(a)$	1	-1	1	1	1	-1	-1	-1	1	-1

a	a^{-1}	$J_{11}(a)$	$J_{11}(a^{-1})$
3	4	1	1
7	8	-1	-1

Legendre symbol of EG key

Fact: Let $p \geq 3$ be a prime and $x, y \in \mathbf{Z}_{p-1}$. Let $X = g^x$ and $Y = g^y$ and $K = g^{xy}$. Then

$$J_p(K) = \begin{cases} 1 & \text{if } J_p(X) = 1 \text{ or } J_p(Y) = 1 \\ -1 & \text{otherwise} \end{cases}$$

In particular one can determine $J_p(K)$ given $J_p(X)$ and $J_p(Y)$

Proof:

$$\begin{aligned} J_p(K) &= J_p(g^{xy}) = \begin{cases} 1 & \text{if } xy \text{ is even} \\ -1 & \text{otherwise} \end{cases} \\ &= \begin{cases} 1 & \text{if } x \text{ is even or } y \text{ is even} \\ -1 & \text{otherwise} \end{cases} \\ &= \begin{cases} 1 & \text{if } J_p(g^x) = 1 \text{ or } J_p(g^y) = 1 \\ -1 & \text{otherwise} \end{cases} \end{aligned}$$

EG modulo a prime

Let p be a prime and g a generator of $\mathbf{Z}_p^*$. The EG PKE scheme $\mathcal{AE}_{\mathrm{EG}} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is defined by

```
**Alg** $\mathcal{K}$
$x \xleftarrow{\$} \mathbf{Z}_{p-1}$
$X \leftarrow g^x$
return $(X, x)$
```

```
**Alg** $\mathcal{E}_X(M)$
$y \xleftarrow{\$} \mathbf{Z}_{p-1}$; $Y \leftarrow g^y$
$K \leftarrow X^y$
$W \leftarrow K \cdot M$
return $(Y, W)$
```

```
**Alg** $\mathcal{D}_x(Y, W)$
$K = Y^x$
$M \leftarrow W \cdot K^{-1}$
return $M$
```

The weakness: Suppose $(Y, W) \xleftarrow{\$} \mathcal{E}_X(M)$. Then we claim that given

- the public key X
- the ciphertext (Y, W)

an adversary can easily compute $J_p(M)$.

This represents a loss of partial information.

EG modulo a prime

Suppose (Y, W) is an encryption of M under public key $X = g^x$, where $Y = g^y$. Then

- $W = K \cdot M$
- $K = g^{xy}$

So

$$\begin{aligned} J_p(M) &= J_p(W \cdot K^{-1}) = J_p(W) \cdot J_p(K^{-1}) = J_p(W) \cdot J_p(K) \\ &= J_p(W) \cdot s \end{aligned}$$

where $s = \begin{cases} 1 & \text{if } J_p(X) = 1 \text{ or } J_p(Y) = 1 \\ -1 & \text{otherwise.} \end{cases}$

So we can compute $J_p(M)$ via

```
Alg FIND-J($X, Y, W$)
if $J_p(X) = 1$ or $J_p(Y) = 1$ then $s \leftarrow 1$ else $s \leftarrow -1$
return $J_p(W) \cdot s$
```

EG modulo a prime

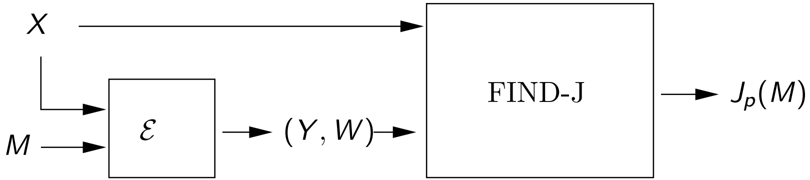
Let p be a prime and g a generator of $\mathbf{Z}_p^*$. The EG PKE scheme $\mathcal{AE}_{\mathrm{EG}} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is defined by

```
**Alg** $\mathcal{K}$
$x \xleftarrow{\$} \mathbf{Z}_{p-1}$
$X \leftarrow g^x$
return $(X, x)$
```

```
**Alg** $\mathcal{E}_X(M)$
$y \xleftarrow{\$} \mathbf{Z}_{p-1}$; $Y \leftarrow g^y$
$K \leftarrow X^y$
$W \leftarrow K \cdot M$
return $(Y, W)$
```

```
**Alg** $\mathcal{D}_x(Y, W)$
$K = Y^x$
$M \leftarrow W \cdot K^{-1}$
return $M$
```

The weakness: There is an algorithm FIND-J



X

M

$\mathcal{E}$

(Y, W)

FIND-J

$J_p(M)$

IND-CPA attack

Given public key X

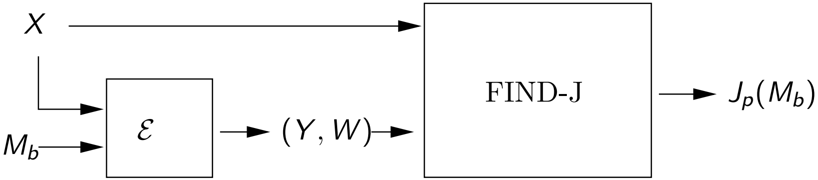
- Produce two messages M_0, M_1
- Receive encryption (Y, W) of M_b
- Figure out b

IND-CPA attack

Given public key X

- Produce two messages M_0, M_1
- Receive encryption (Y, W) of M_b
- Figure out b

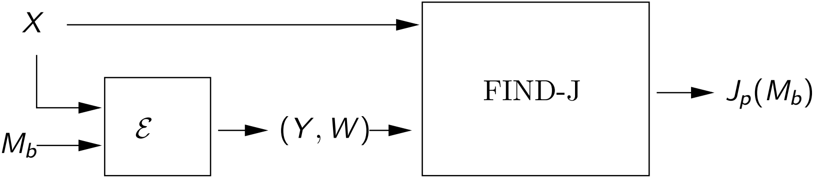
How? Use:



IND-CPA attack

Given public key X

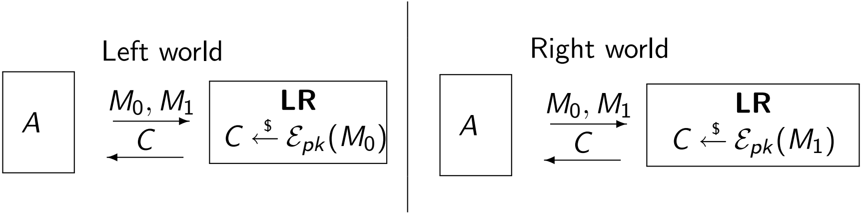
- Let M_0, M_1 be such that $J_p(M_0) = -1$ and $J_p(M_1) = 1$
- Receive encryption (Y, W) of M_b



- if $\text{FIND-J}(X, Y, W) = 1$ then return 1 else return 0

IND-CPA attack on EG

Let $\mathcal{AE}_{\mathrm{EG}} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be the EG PKE scheme over $\mathbf{Z}_p^*$ where p is a prime.



Left world

A

M_0, M_1

C

LR

$C \xleftarrow{\$} \mathcal{E}_{pk}(M_0)$

Right world

A

M_0, M_1

C

LR

$C \xleftarrow{\$} \mathcal{E}_{pk}(M_1)$

```
adversary A(X)
$M_1 \leftarrow 1 \,;\; M_0 \leftarrow g$
$(Y, W) \xleftarrow{\$} \mathbf{LR}(M_0, M_1)$
if $\mathrm{FIND\text{-}J}(X, Y, W) = 1$ then return 1 else return 0
```

Then

$$\begin{aligned}\mathbf{Adv}^{\mathrm{ind\text{-}cpa}}_{\mathcal{AE}_{\mathrm{EG}},A} &= \Pr\left[\mathrm{Right}^{A}_{\mathcal{AE}_{\mathrm{EG}}} \Rightarrow 1\right] - \Pr\left[\mathrm{Left}^{A}_{\mathcal{AE}_{\mathrm{EG}}} \Rightarrow 1\right] \\ &= 1 - 0 = 1\end{aligned}$$

IND-CPA security of EG

We have seen that EG is not IND-CPA over groups $G = \mathbf{Z}_p^*$ for prime p.

However it is IND-CPA secure over any group G where the DDH problem is hard.

This is not a contradiction because if p is prime then the DDH problem in $\mathbf{Z}_p^*$ is easy even though DL, CDH seem to be hard.

We can in particular securely implement EG over

- Appropriate prime-order subgroups of $\mathbf{Z}_p^*$ for a prime p
- Elliptic curve groups of prime order

Message encoding in $\mathcal{AE}_{\mathrm{EG}}$

The $\mathcal{AE}_{\mathrm{EG}}$ asymmetric encryption scheme assumes that messages can be encoded as elements of the underlying group G. But

- Messages may be of large and varying lengths, but we want the group to be fixed beforehand and as small as possible
- For some groups this encoding is hard even if the messages are short

Speed

Asymmetric cryptography is orders of magnitude slower than symmetric cryptography

An exponentiation in a 160-bit elliptic curve group costs about the same as 3000-4000 hashes or block cipher operations

Hybrid encryption

Build an asymmetric encryption scheme by combining symmetric and asymmetric techniques:

- Symmetrically encrypt data under a key K
- Asymmetrically encrypt K

Benefits:

- Speed
- No encoding problems

EG again

Let $G = \langle g \rangle$ be a cyclic group of order m and let $sk = x$ and $pk = X = g^x$ be $\mathcal{AE}_{\mathrm{EG}}$ keys.

```
**Alg** $\mathcal{E}_X(M)$
$y \xleftarrow{\$} \mathbf{Z}_{p-1}$; $Y \leftarrow g^y$
$K \leftarrow X^y$
$W \leftarrow K \cdot M$
return $(Y, W)$
```

In EG, the "symmetric key" is K and it "symmetrically" encrypts M as $W = K \cdot M$.

An alternative to $\mathcal{AE}_{\mathrm{EG}}$

Let the "symmetric key" be $K = H(g^{y} \parallel g^{xy})$ rather than merely g^{xy}, where $H\colon \{0,1\}^{*} \to \{0,1\}^{k}$ is a hash function.

Instead of $K \cdot M$, let W be an encryption of M under K with some known-secure symmetric scheme such as AES-CBC. In this case $k = 128$ above.

DHIES [ABR]

Let $G = \langle g \rangle$ be a cyclic group of order m, H: $\{0,1\}^* \to \{0,1\}^k$ a hash function, and $\mathcal{SE} = (\mathcal{KS}, \mathcal{ES}, \mathcal{DS})$ a symmetric encryption scheme with k-bit keys. Then DHIES is $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ where

```
**Alg** $\mathcal{K}$
$x \xleftarrow{\$} \mathbf{Z}_m$
$X \leftarrow g^x$
return $(X, x)$
```

```
**Alg** $\mathcal{E}_X(M)$
$y \xleftarrow{\$} \mathbf{Z}_m$ ; $Y \leftarrow g^y$
$Z \leftarrow X^y$
$K \leftarrow H(Y \| Z)$
$C_s \xleftarrow{\$} \mathcal{ES}_K(M)$
return $(Y, C_s)$
```

```
**Alg** $\mathcal{D}_x(Y, C_s)$
$Z \leftarrow Y^x$
$K \leftarrow H(Y \| Z)$
$M \xleftarrow{\$} \mathcal{DS}_K(C_s)$
return $M$
```

ECIES

ECIES is DHIES when G is an elliptic curve group.

Operation	**Cost**
encryption	2 160-bit exp
decryption	1 160-bit exp
ciphertext expansion	160-bits

ciphertext expansion = (length of ciphertext) - (length of plaintext)

RSA Math

Recall that $\varphi(N) = |\mathbf{Z}_N^*|$.

Claim: Suppose $e, d \in \mathbf{Z}_{\varphi(N)}^*$ satisfy $ed \equiv 1 \pmod{\varphi(N)}$. Then for any $x \in \mathbf{Z}_N^*$ we have

$$(x^e)^d \equiv x \pmod{N}$$

Proof:

$$(x^e)^d \equiv x^{ed \bmod \varphi(N)} \equiv x^1 \equiv x$$

modulo N

The RSA function

A modulus N and encryption exponent e define the RSA function $f : \mathbf{Z}_N^* \to \mathbf{Z}_N^*$ defined by

$$f(x) = x^e \mod N$$

for all $x \in \mathbf{Z}_N^*$.

A value $d \in Z_{\varphi(N)}^*$ satisfying $ed \equiv 1 \pmod{\varphi(N)}$ is called a decryption exponent.

Claim: The RSA function $f : \mathbf{Z}_N^* \to \mathbf{Z}_N^*$ is a permutation with inverse $f^{-1} : \mathbf{Z}_N^* \to \mathbf{Z}_N^*$ given by

$$f^{-1}(y) = y^d \mod N$$

Proof: For all $x \in \mathbf{Z}_N^*$ we have

$$f^{-1}(f(x)) \equiv (x^e)^d \equiv x \pmod{N}$$

by previous claim.

Example

Let $N = 15$. So

$$\begin{aligned}\mathbf{Z}_N^* &= \{1, 2, 4, 7, 8, 11, 13, 14\} \\ \varphi(N) &=\end{aligned}$$

Example

Let $N = 15$. So

$$\begin{aligned} \mathbf{Z}_N^* &= \{1, 2, 4, 7, 8, 11, 13, 14\} \\ \varphi(N) &= 8 \\ \mathbf{Z}_{\varphi(N)}^* &= \{1, 3, 5, 7\} \end{aligned}$$

Let $e = 3$ and $d = 3$. Then

$$ed \equiv 9 \equiv 1 \pmod 8$$

Let

$$\begin{aligned} f(x) &= x^3 \bmod 15 \\ g(y) &= y^3 \bmod 15 \end{aligned}$$

x	$f(x)$	$g(f(x))$
1	1	
2	8	
4		
7		
8		
11		
13		
14		

Example

Let $N = 15$. So

$$\begin{aligned}\mathbf{Z}_N^* &= \{1, 2, 4, 7, 8, 11, 13, 14\} \\ \varphi(N) &= 8 \\ \mathbf{Z}_{\varphi(N)}^* &= \{1, 3, 5, 7\}\end{aligned}$$

Let $e = 3$ and $d = 3$. Then

$$ed \equiv 9 \equiv 1 \pmod 8$$

Let

$$\begin{aligned}f(x) &= x^3 \bmod 15 \\ g(y) &= y^3 \bmod 15\end{aligned}$$

x	$f(x)$	$g(f(x))$
1	1	
2	8	
4	4	
7		
8		
11		
13		
14		

Example

Let $N = 15$. So

$$\begin{aligned} \mathbf{Z}_N^* &= \{1, 2, 4, 7, 8, 11, 13, 14\} \\ \varphi(N) &= 8 \\ \mathbf{Z}_{\varphi(N)}^* &= \{1, 3, 5, 7\} \end{aligned}$$

Let $e = 3$ and $d = 3$. Then

$$ed \equiv 9 \equiv 1 \pmod 8$$

Let

$$\begin{aligned} f(x) &= x^3 \bmod 15 \\ g(y) &= y^3 \bmod 15 \end{aligned}$$

x	$f(x)$	$g(f(x))$
1	1	
2	8	
4	4	
7	13	
8		
11		
13		
14		

Example

Let $N = 15$. So

$$\begin{aligned} \mathbf{Z}_N^* &= \{1, 2, 4, 7, 8, 11, 13, 14\} \\ \varphi(N) &= 8 \\ \mathbf{Z}_{\varphi(N)}^* &= \{1, 3, 5, 7\} \end{aligned}$$

Let $e = 3$ and $d = 3$. Then

$$ed \equiv 9 \equiv 1 \pmod 8$$

Let

$$\begin{aligned} f(x) &= x^3 \bmod 15 \\ g(y) &= y^3 \bmod 15 \end{aligned}$$

x	$f(x)$	$g(f(x))$
1	1	
2	8	
4	4	
7	13	
8	2	
11		
13		
14		

Example

Let $N = 15$. So

$$\begin{aligned} \mathbf{Z}_N^* &= \{1, 2, 4, 7, 8, 11, 13, 14\} \\ \varphi(N) &= 8 \\ \mathbf{Z}_{\varphi(N)}^* &= \{1, 3, 5, 7\} \end{aligned}$$

Let $e = 3$ and $d = 3$. Then

$$ed \equiv 9 \equiv 1 \pmod 8$$

Let

$$\begin{aligned} f(x) &= x^3 \bmod 15 \\ g(y) &= y^3 \bmod 15 \end{aligned}$$

x	$f(x)$	$g(f(x))$
1	1	
2	8	
4	4	
7	13	
8	2	
11	11	
13		
14		

Example

Let $N = 15$. So

$$\begin{aligned} \mathbf{Z}_N^* &= \{1, 2, 4, 7, 8, 11, 13, 14\} \\ \varphi(N) &= 8 \\ \mathbf{Z}_{\varphi(N)}^* &= \{1, 3, 5, 7\} \end{aligned}$$

Let $e = 3$ and $d = 3$. Then

$$ed \equiv 9 \equiv 1 \pmod 8$$

Let

$$\begin{aligned} f(x) &= x^3 \bmod 15 \\ g(y) &= y^3 \bmod 15 \end{aligned}$$

x	$f(x)$	$g(f(x))$
1	1	
2	8	
4	4	
7	13	
8	2	
11	11	
13	7	
14		

Example

Let $N = 15$. So

$$\begin{aligned} \mathbf{Z}_N^* &= \{1, 2, 4, 7, 8, 11, 13, 14\} \\ \varphi(N) &= 8 \\ \mathbf{Z}_{\varphi(N)}^* &= \{1, 3, 5, 7\} \end{aligned}$$

Let $e = 3$ and $d = 3$. Then

$$ed \equiv 9 \equiv 1 \pmod 8$$

Let

$$\begin{aligned} f(x) &= x^3 \bmod 15 \\ g(y) &= y^3 \bmod 15 \end{aligned}$$

x	$f(x)$	$g(f(x))$
1	1	
2	8	
4	4	
7	13	
8	2	
11	11	
13	7	
14	14	

Example

Let $N = 15$. So

$$\begin{aligned} \mathbf{Z}_N^* &= \{1, 2, 4, 7, 8, 11, 13, 14\} \\ \varphi(N) &= 8 \\ \mathbf{Z}_{\varphi(N)}^* &= \{1, 3, 5, 7\} \end{aligned}$$

Let $e = 3$ and $d = 3$. Then

$$ed \equiv 9 \equiv 1 \pmod 8$$

Let

$$\begin{aligned} f(x) &= x^3 \bmod 15 \\ g(y) &= y^3 \bmod 15 \end{aligned}$$

x	$f(x)$	$g(f(x))$
1	1	1
2	8	
4	4	
7	13	
8	2	
11	11	
13	7	
14	14	

Example

Let $N = 15$. So

$$\begin{aligned}
\mathbf{Z}_N^* &= \{1, 2, 4, 7, 8, 11, 13, 14\} \\
\varphi(N) &= 8 \\
\mathbf{Z}_{\varphi(N)}^* &= \{1, 3, 5, 7\}
\end{aligned}$$

Let $e = 3$ and $d = 3$. Then

$$ed \equiv 9 \equiv 1 \pmod{8}$$

Let

$$\begin{aligned}
f(x) &= x^3 \bmod 15 \\
g(y) &= y^3 \bmod 15
\end{aligned}$$

x	$f(x)$	$g(f(x))$
1	1	1
2	8	2
4	4	
7	13	
8	2	
11	11	
13	7	
14	14	

Example

Let $N = 15$. So

$$\begin{aligned} \mathbf{Z}_N^* &= \{1, 2, 4, 7, 8, 11, 13, 14\} \\ \varphi(N) &= 8 \\ \mathbf{Z}_{\varphi(N)}^* &= \{1, 3, 5, 7\} \end{aligned}$$

Let $e = 3$ and $d = 3$. Then

$$ed \equiv 9 \equiv 1 \pmod 8$$

Let

$$\begin{aligned} f(x) &= x^3 \bmod 15 \\ g(y) &= y^3 \bmod 15 \end{aligned}$$

x	$f(x)$	$g(f(x))$
1	1	1
2	8	2
4	4	4
7	13	
8	2	
11	11	
13	7	
14	14	

Example

Let $N = 15$. So

$$\begin{aligned}\mathbf{Z}_N^* &= \{1,2,4,7,8,11,13,14\} \\ \varphi(N) &= 8 \\ \mathbf{Z}_{\varphi(N)}^* &= \{1,3,5,7\}\end{aligned}$$

Let $e = 3$ and $d = 3$. Then

$$ed \equiv 9 \equiv 1 \pmod 8$$

Let

$$\begin{aligned}f(x) &= x^3 \bmod 15 \\ g(y) &= y^3 \bmod 15\end{aligned}$$

x	$f(x)$	$g(f(x))$
1	1	1
2	8	2
4	4	4
7	13	7
8	2	
11	11	
13	7	
14	14	

Example

Let $N = 15$. So

$$\begin{aligned} \mathbf{Z}_N^* &= \{1,2,4,7,8,11,13,14\} \\ \varphi(N) &= 8 \\ \mathbf{Z}_{\varphi(N)}^* &= \{1,3,5,7\} \end{aligned}$$

Let $e = 3$ and $d = 3$. Then

$$ed \equiv 9 \equiv 1 \pmod 8$$

Let

$$\begin{aligned} f(x) &= x^3 \bmod 15 \\ g(y) &= y^3 \bmod 15 \end{aligned}$$

x	$f(x)$	$g(f(x))$
1	1	1
2	8	2
4	4	4
7	13	7
8	2	8
11	11	
13	7	
14	14	

Example

Let $N = 15$. So

$$\begin{aligned}
\mathbf{Z}_N^* &= \{1, 2, 4, 7, 8, 11, 13, 14\} \\
\varphi(N) &= 8 \\
\mathbf{Z}_{\varphi(N)}^* &= \{1, 3, 5, 7\}
\end{aligned}$$

Let $e = 3$ and $d = 3$. Then

$$ed \equiv 9 \equiv 1 \pmod 8$$

Let

$$\begin{aligned}
f(x) &= x^3 \bmod 15 \\
g(y) &= y^3 \bmod 15
\end{aligned}$$

x	$f(x)$	$g(f(x))$
1	1	1
2	8	2
4	4	4
7	13	7
8	2	8
11	11	11
13	7	
14	14	

Example

Let $N = 15$. So

$$\begin{aligned} \mathbf{Z}_N^* &= \{1, 2, 4, 7, 8, 11, 13, 14\} \\ \varphi(N) &= 8 \\ \mathbf{Z}_{\varphi(N)}^* &= \{1, 3, 5, 7\} \end{aligned}$$

Let $e = 3$ and $d = 3$. Then

$$ed \equiv 9 \equiv 1 \pmod 8$$

Let

$$\begin{aligned} f(x) &= x^3 \bmod 15 \\ g(y) &= y^3 \bmod 15 \end{aligned}$$

x	$f(x)$	$g(f(x))$
1	1	1
2	8	2
4	4	4
7	13	7
8	2	8
11	11	11
13	7	13
14	14	

Example

Let $N = 15$. So

$$\begin{aligned} \mathbf{Z}_N^* &= \{1, 2, 4, 7, 8, 11, 13, 14\} \\ \varphi(N) &= 8 \\ \mathbf{Z}_{\varphi(N)}^* &= \{1, 3, 5, 7\} \end{aligned}$$

Let $e = 3$ and $d = 3$. Then

$$ed \equiv 9 \equiv 1 \pmod 8$$

Let

$$\begin{aligned} f(x) &= x^3 \bmod 15 \\ g(y) &= y^3 \bmod 15 \end{aligned}$$

x	$f(x)$	$g(f(x))$
1	1	1
2	8	2
4	4	4
7	13	7
8	2	8
11	11	11
13	7	13
14	14	14

RSA usage

- $pk = N, e;\ \ sk = N, d$
- $\mathcal{E}_{pk}(x) = x^e \mod N = f(x)$
- $\mathcal{D}_{sk}(y) = y^d \mod N = f^{-1}(y)$

Security will rely on it being hard to compute f^{-1} without knowing d.

RSA is a trapdoor, one-way permutation:

- Easy to invert given trapdoor d
- Hard to invert given only N, e

RSA generators

An RSA generator with security parameter k is an algorithm $\mathcal{K}_{rsa}$ that returns N, p, q, e, d satisfying

- p, q are distinct odd primes
- $N = pq$ and is called the (RSA) modulus
- $|N| = k$, meaning $2^{k-1} \leq N \leq 2^k$
- $e \in \mathbf{Z}^*_{\varphi(N)}$ is called the encryption exponent
- $d \in \mathbf{Z}^*_{\varphi(N)}$ is called the decryption exponent
- $ed \equiv 1 \pmod{\varphi(N)}$

Plan

- Building RSA generators
- Basic RSA security
- Encryption with RSA

Some more math

Fact: If p, q are distinct primes and $N = pq$ then $\varphi(N) = (p-1)(q-1)$.

Proof:

$$\begin{aligned}\varphi(N) &= |\{1,\dots,N-1\}| - |\{ip : 1 \leq i \leq q-1\}| - |\{iq : 1 \leq i \leq p-1\}| \\ &= (N-1) - (q-1) - (p-1) \\ &= N - p - q + 1 \\ &= pq - p - q + 1 \\ &= (p-1)(q-1)\end{aligned}$$

Example:

- $15 = 3 \cdot 5$
- $\mathbf{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$
- $\varphi(15) = 8 = (3-1)(5-1)$

Recall

Given $\varphi(N)$ and $e \in \mathbf{Z}^*_{\varphi(N)}$, we can compute $d \in \mathbf{Z}^*_{\varphi(N)}$ satisfying $ed \equiv 1 \pmod{\varphi(N)}$ via

$$d \leftarrow \mathrm{MOD\text{-}INV}(e, \varphi(N)).$$

We have algorithms to efficiently test whether a number is prime, and a random number has a pretty good chance of being a prime.

Building RSA generators

Say we wish to have $e = 3$ (for efficiency). The generator $\mathcal{K}_{rsa}^{3}$ with (even) security parameter k:

```
repeat
    $p, q \xleftarrow{\$} \{2^{k/2-1}, \ldots, 2^{k/2} - 1\}$; $N \leftarrow pq$; $M \leftarrow (p-1)(q-1)$
until
    $N \geq 2^{k-1}$ and $p, q$ are prime and $gcd(e, M) = 1$
$d \leftarrow \mathrm{MOD\text{-}INV}(e, M)$
return $N, p, q, e, d$
```

One-wayness of RSA

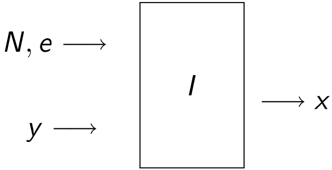
The following should be hard:

Given: N, e, y where $y = f(x) = x^e \mod N$

Find: x

Formalism picks x at random and generates N, e via an RSA generator.

ow-adversaries



$N, e \longrightarrow$

$y \longrightarrow$

I

$\longrightarrow x$

wins if $x = f^{-1}(y)$, meaning $x^e \equiv y \pmod{N}$.

One-wayness of RSA, formally

Let K_{rsa} be a RSA generator and I an adversary.

Game $\mathrm{OW}_{K_{rsa}}$

```
procedure Initialize
$(N, p, q, e, d) \xleftarrow{\$} K_{rsa}$
$x \xleftarrow{\$} \mathbf{Z}_N^*$; $y \leftarrow x^e \mod N$
return $N, e, y$

procedure Finalize$(x')$
return $(x = x')$
```

The ow-advantage of I is

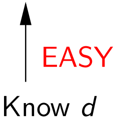
$$\mathbf{Adv}^{\mathrm{ow}}_{K_{rsa}}(I) = \Pr\left[\mathrm{OW}^{I}_{K_{rsa}} \Rightarrow \text{true}\right]$$

Inverting RSA

Inverting RSA : given N, e, y find x such that $x^e \equiv y \pmod{N}$

Inverting RSA

Inverting RSA : given N, e, y find x such that $x^e \equiv y \pmod{N}$

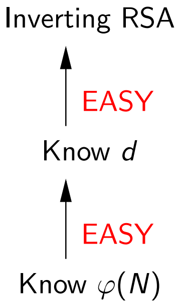


EASY

because $f^{-1}(y) = y^d \bmod N$

Know d

Inverting RSA



Inverting RSA : given N, e, y find x such that $x^e \equiv y \pmod{N}$

EASY because $f^{-1}(y) = y^d \bmod N$

Know d

EASY because $d = e^{-1} \bmod \varphi(N)$

Know $\varphi(N)$

Inverting RSA

Inverting RSA : given N, e, y find x such that $x^e \equiv y \pmod{N}$

↑ EASY because $f^{-1}(y) = y^d \bmod N$

Know d

↑ EASY because $d = e^{-1} \bmod \varphi(N)$

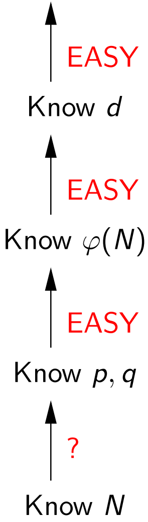
Know $\varphi(N)$

↑ EASY because $\varphi(N) = (p-1)(q-1)$

Know p, q

Inverting RSA

Inverting RSA : given N, e, y find x such that $x^e \equiv y \pmod{N}$



EASY because $f^{-1}(y) = y^d \bmod N$

Know d

EASY because $d = e^{-1} \bmod \varphi(N)$

Know $\varphi(N)$

EASY because $\varphi(N) = (p-1)(q-1)$

Know p, q

?

Know N

Factoring Problem

Given: N where $N = pq$ and p, q are prime

Find: p, q

If we can factor we can invert RSA. We do not know whether the converse is true, meaning whether or not one can invert RSA without factoring.

A factoring algorithm

```
**Alg** FACTOR($N$)    // $N = pq$ where $p, q$ are primes
for $i = 2, \ldots, \left\lceil \sqrt{N} \right\rceil$ do
  if $N \bmod i = 0$ then
    $p \leftarrow i$ ; $q \leftarrow N/i$ ; return $p, q$
```

This algorithm works but takes time

$$\mathcal{O}(\sqrt{N}) = \mathcal{O}(e^{0.5 \ln N})$$

which is prohibitive.

Factoring algorithms

Algorithm	**Time taken to factor N**
Naive	$O(e^{0.5 \ln N})$
Quadratic Sieve (QS)	$O(e^{c(\ln N)^{1/2}(\ln \ln N)^{1/2}})$
Number Field Sieve (NFS)	$O(e^{1.92(\ln N)^{1/3}(\ln \ln N)^{2/3}})$

Factoring records

Number	**bit-length**	**Factorization**	**alg**	**MIPS years**
RSA-400	400	1993	QS	830
RSA-428	428	1994	QS	5000
RSA-431	431	1996	NFS	1000
RSA-465	465	1999	NFS	2000
RSA-515	515	1999	NFS	8000
RSA-576	576	2003	NFS	

How big is big enough?

Current wisdom: For 80-bit security, use a 1024 bit RSA modulus

80-bit security: Factoring takes 2^{80} time.

Factorization of RSA-1024 seems out of reach at present.

Estimates vary, and for more security, longer moduli are recommended.

RSA: what to remember

The RSA function $f(x) = x^e \mod N$ is a trapdoor one way permutation:

- Easy forward: given N, e, x it is easy to compute $f(x)$
- Easy back with trapdoor: Given N, d and $y = f(x)$ it is easy to compute $x = f^{-1}(y) = y^d \mod N$
- Hard back without trapdoor: Given N, e and $y = f(x)$ it is hard to compute $x = f^{-1}(y)$

Plain-RSA encryption

The plain RSA asymmetric encryption scheme $\mathcal{AE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ associated to RSA generator K_{rsa} is

```
Alg $\mathcal{K}$
$(N, p, q, e, d) \xleftarrow{\$} K_{rsa}$
$pk \leftarrow (N, e)$
$sk \leftarrow (N, d)$
return $(pk, sk)$
```

```
Alg $\mathcal{E}_{pk}(M)$
$C \leftarrow M^e \mod N$
return $C$
```

```
Alg $\mathcal{D}_{sk}(C)$
$M \leftarrow C^d \mod N$
return $M$
```

The "easy-back with trapdoor" property implies

$$\mathcal{D}_{sk}(\mathcal{E}_{pk}(M)) = M$$

for all $M \in \mathbf{Z}_N^*$.

Plain-RSA encryption security

```
Alg $\mathcal{K}$
$(N, p, q, e, d) \xleftarrow{\$} K_{rsa}$
$pk \leftarrow (N, e)$
$sk \leftarrow (N, d)$
return $(pk, sk)$
```

```
Alg $\mathcal{E}_{pk}(M)$
$C \leftarrow M^e \mod N$
return $C$
```

```
Alg $\mathcal{D}_{sk}(C)$
$M \leftarrow C^d \mod N$
return $M$
```

Getting *sk* from *pk* involves factoring N.

Plain-RSA encryption security

```
Alg $\mathcal{K}$
$(N, p, q, e, d) \xleftarrow{\$} K_{rsa}$
$pk \leftarrow (N, e)$
$sk \leftarrow (N, d)$
return $(pk, sk)$
```

```
Alg $\mathcal{E}_{pk}(M)$
$C \leftarrow M^e \mod N$
return $C$
```

```
Alg $\mathcal{D}_{sk}(C)$
$M \leftarrow C^d \mod N$
return $M$
```

Alg $\mathcal{E}$ is deterministic so we can detect repeats and the scheme is not IND-CPA secure.

A message recovery attack

Suppose sender encrypts M and $M+1$ under public key $N, 3$. Adversary has

$$C_1 = M^3 \mod N \text{ and } C_2 = (M+1)^3 \mod N$$

Then modulo N we have

$$\frac{C_2 + 2C_1 - 1}{C_2 - C_1 + 2} \quad =$$

A message recovery attack

Suppose sender encrypts M and $M+1$ under public key $N, 3$. Adversary has

$$C_1 = M^3 \mod N \text{ and } C_2 = (M+1)^3 \mod N$$

Then modulo N we have

$$\begin{aligned} \frac{C_2 + 2C_1 - 1}{C_2 - C_1 + 2} &= \frac{(M+1)^3 + 2M^3 - 1}{(M+1)^3 - M^3 + 2} \\ &= \end{aligned}$$

A message recovery attack

Suppose sender encrypts M and $M+1$ under public key $N,3$. Adversary has

$$C_1 = M^3 \mod N \text{ and } C_2 = (M+1)^3 \mod N$$

Then modulo N we have

$$\begin{aligned} \frac{C_2 + 2C_1 - 1}{C_2 - C_1 + 2} &= \frac{(M+1)^3 + 2M^3 - 1}{(M+1)^3 - M^3 + 2} \\ &= \frac{(M^3 + 3M^2 + 3M + 1) + 2M^3 - 1}{(M^3 + 3M^2 + 3M + 1) - M^3 + 2} \\ &= \end{aligned}$$

A message recovery attack

Suppose sender encrypts M and $M+1$ under public key $N, 3$. Adversary has

$$C_1 = M^3 \mod N \text{ and } C_2 = (M+1)^3 \mod N$$

Then modulo N we have

$$\begin{aligned}\frac{C_2 + 2C_1 - 1}{C_2 - C_1 + 2} &= \frac{(M+1)^3 + 2M^3 - 1}{(M+1)^3 - M^3 + 2} \\ &= \frac{(M^3 + 3M^2 + 3M + 1) + 2M^3 - 1}{(M^3 + 3M^2 + 3M + 1) - M^3 + 2} \\ &= \frac{3M^3 + 3M^2 + 3M}{3M^2 + 3M + 3} =\end{aligned}$$

A message recovery attack

Suppose sender encrypts M and $M+1$ under public key $N, 3$. Adversary has

$$C_1 = M^3 \mod N \text{ and } C_2 = (M+1)^3 \mod N$$

Then modulo N we have

$$\begin{aligned}\frac{C_2 + 2C_1 - 1}{C_2 - C_1 + 2} &= \frac{(M+1)^3 + 2M^3 - 1}{(M+1)^3 - M^3 + 2} \\ &= \frac{(M^3 + 3M^2 + 3M + 1) + 2M^3 - 1}{(M^3 + 3M^2 + 3M + 1) - M^3 + 2} \\ &= \frac{3M^3 + 3M^2 + 3M}{3M^2 + 3M + 3} = \frac{M(3M^2 + 3M + 3)}{3M^2 + 3M + 3} = M\end{aligned}$$

so adversary an recover M.

The SRSA scheme

Encrypt M unde $pk = N, e$ via:

- $x \xleftarrow{\$} \mathbf{Z}_N^*$; $C_a \leftarrow x^e$ mod N;
- $K \leftarrow H(x)$
- Let C_s be a symmetric encryption of M under K
- Ciphertext is (C_a, C_s)

Decrypt (C_a, C_S) under $sk = N, d$ via:

- $x \leftarrow C_a^d$ mod N
- $K \leftarrow H(x)$
- Decrypt C_s under K to get M

The SRSA scheme

Let $\mathcal{SE} = (\mathcal{KS}, \mathcal{ES}, \mathcal{DS})$ be a symmetric encryption scheme with k-bit keys, and $H\colon \{0,1\}^* \to \{0,1\}^k$ a hash function.

Example: $\mathcal{SE}$ could be AES CBC encryption in which case $k = 128$.

The SRSA asymmetric encryption scheme $\mathcal{AE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ associated to RSA generator K_{rsa} is

```
**Alg** $\mathcal{K}$
$(N, p, q, e, d) \xleftarrow{\$} K_{rsa}$
$pk \leftarrow (N, e)$
$sk \leftarrow (N, d)$
return $(pk, sk)$
```

```
**Alg** $\mathcal{E}_{N,e}(M)$
$x \xleftarrow{\$} \mathbf{Z}_N^*$
$K \leftarrow H(x)$
$C_a \leftarrow x^e \bmod N$
$C_s \xleftarrow{\$} \mathcal{ES}_K(M)$
return $(C_a, C_s)$
```

```
**Alg** $\mathcal{E}_{N,d}(C_a, C_s)$
$x \leftarrow C_a^d \bmod N$
$K \leftarrow H(x)$
$M \leftarrow \mathcal{DS}_K(C_s)$
return $M$
```

PKCS #1

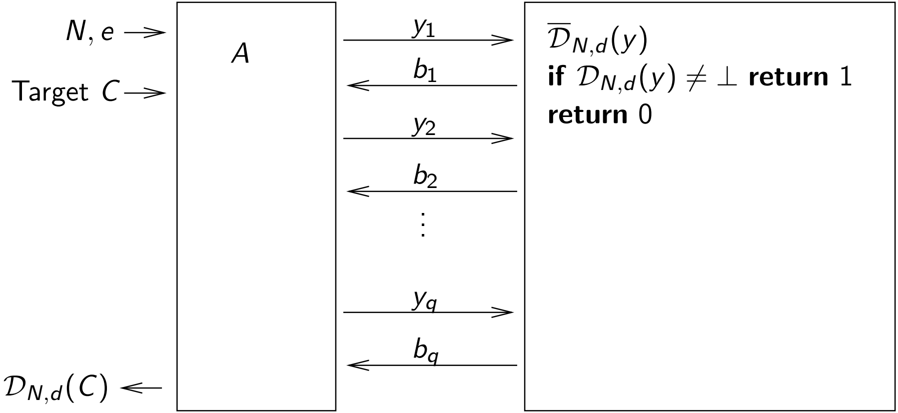
Receiver keys: $pk = (N, e)$ and $sk = (N, d)$ where $n = |N|_8 = 128$

```
**Alg** $\mathcal{E}_{N,e}(M)$    $// \; m = |M|_8 \leq n - 11$
$Pad \xleftarrow{\$} (\{0,1\}^8 - \{00\})^{n-m-3}$
$x \leftarrow 00||02||Pad||00||M$
$C \leftarrow x^e \bmod N$
**return** $C$
```

```
**Alg** $\mathcal{D}_{N,d}(C)$    $// \; C \in \mathbb{Z}_N^*$
$x \leftarrow C^d \bmod N$
$aa||bb||w \leftarrow x$
**if** $aa \neq 00$ or $bb \neq 02$ or $00 \notin w$ **then**
    **return** $\perp$
$Pad||00||M \leftarrow w$ where $00 \notin Pad$
**return** $M$
```

$$x = \begin{array}{|c|c|c|c|c|}\hline 00 & 02 & Pad & 00 & M \\ \hline \end{array}$$

Attack on PKCS #1 [Bl98]



$N, e \rightarrow$

Target $C \rightarrow$

A

$\xrightarrow{y_1}$

$\xleftarrow{b_1}$

$\xrightarrow{y_2}$

$\xleftarrow{b_2}$

$\vdots$

$\xrightarrow{y_q}$

$\xleftarrow{b_q}$

$\mathcal{D}_{N,d}(C) \leftarrow$

```
$\overline{\mathcal{D}}_{N,d}(y)$
if $\mathcal{D}_{N,d}(y) \neq \perp$ return 1
return 0
```

The attack A succeeds in decrypting C after making $q \approx 1$ million clever queries to the box.

Attack on PKCS #1 and response

This is a (limited) chosen-ciphertext attack in which the oracle does not fully decrypt but indicates whether or not the decryption is valid.

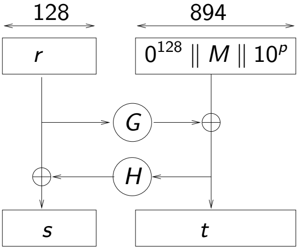
The attack can be mounted on SSL.

Use of an IND-CCA scheme would prevent the attack.

OAEP [BR94]

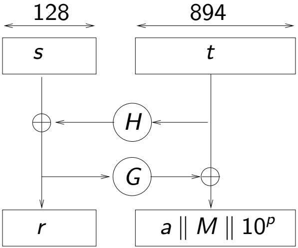
Receiver keys: $pk = (N, e)$ and $sk = (N, d)$ where $|N| = 1024$
Hash functions: $G\colon \{0,1\}^{128} \rightarrow \{0,1\}^{894}$ and $H\colon \{0,1\}^{894} \rightarrow \{0,1\}^{128}$

```
Algorithm $\mathcal{E}_{N,e}(M)$    // $|M| \leq 765$
$r \xleftarrow{\$} \{0,1\}^{128}$; $p \leftarrow 765 - |M|$
```



```
$x \leftarrow s||t$
$C \leftarrow x^e \bmod N$
return $C$
```

```
Algorithm $\mathcal{D}_{N,d}(C)$    // $C \in \mathbb{Z}_N^*$
$x \leftarrow C^d \bmod N$
$s||t \leftarrow x$
```



```
if $a = 0^{128}$ then return $M$
else return $\perp$
```

RSA OAEP usage

Protocols:

- SSL ver. 2.0, 3.0 / TLS ver. 1.0, 1.1
- SSH ver 1.0, 2.0
- . . .

Standards:

- RSA PKCS #1 versions 1.5, 2.0
- IEEE P1363
- NESSIE (Europe)
- CRYPTREC (Japan)
- . . .