Introduction to Public-Key Cryptosystems:

- **Technical Underpinnings: RSA and Primality Testing**
- **Modes of Encryption for RSA**
- **Digital Signatures for RSA**

RSA Block Encryption / Decryption and Signing

- Each principal has *private* and *public* values
  - for encryption/decryption
  - for signing

Bob

e, e' public

d, d' private

n = modulus

$\xleftarrow{\{m\}^e}$

Alice

knows e, e'

n = modulus

- **Bob** decrypts block $\{m\}^e$ using d:

  $\left\{\{m\}^e\right\}^d = m$

- **Alice** encrypts block m using e :

  $\{m\}^e$

$\xrightarrow{m,\ \{m\}^{d'}}$

- **Bob** signs block m using d':

  $\{m\}^{d'}$

- **Alice** verifies $\{m\}^{d'}$ using e' :

  $\left\{\{m\}^{d'}\right\}^{e'} = m$

- all operations are mod n, $0 < m < n$

I. Technical Underpinnings

- Common Divisor; Greatest Common Divisor
- Relative Primes
- Modular Arithmetic
- Euclid's Algorithm
- $\mathbf{Z}^*_\mathbf{n}$
- Euler's Totient Function
- Euler's Theorem
- Generalization of Euler's Theorem
- RSA Block Encryption/Decryption and Signing: choosing e and d
- Choosing p and q: Primality Tests
- Miller-Rabin Test

Common Divisor

Definition: *a divides b,* or $a \mid b$, for $a, b \in \mathbf{Z}$, $\mathbf{Z} = \{0, \pm 1, \pm 2 \ldots\}$,
iff there exists $k \in \mathbf{Z}$, such that $a \cdot k = b$

Properties:

- Linearity: if $a \mid b$ and $a \mid c$, then $a \mid (x \cdot b + y \cdot c)$ for any $x, y \in \mathbf{Z}$
- If $d \mid n$, $n \neq 0$, then $|d| \leq |n|$

Definition: c is a *common divisor* of a and b if $c \mid a$ and $c \mid b$

Theorem: For any $a, b \in \mathbf{Z}$, there is *common divisor* d that can be expressed $d = x \cdot a + y \cdot b$, for some $x, y \in \mathbf{Z}$. Furthermore, any other common divisor of a and b also divides d.

Proof [Common Divisor Theorem]:

Choose $a, b \geq 0$ and denote $n = a + b$. Use induction on n

Base Case: $n = 0$ then $a = 0$ and $b = 0$ choose $d = 0$

Hypothesis: assume the assertion holds for $0 \ldots n$-1

Induction Step: From hypothesis, we show it holds for n

$n = a + b$

- if $b = 0$, then $n = a$, choose $d = 1 \cdot a + 0 \cdot b = a$
- if $b \geq 0$, and $b < a$

Consider $(a - b)$ and b

$n' = (a - b) + b = a < n$, so the hypothesis must hold for n', $(a - b)$ and b; i.e., there is a d s.t. $d \mid (a - b)$ and $d \mid b$ and

$$d = x \cdot b + y \cdot (a - b)$$

Proof [Common Divisor Theorem] (ctnd.)

We now show that this same d also divides a:

from linearity $d \mid [b + (a - b)] = d \mid a$

d can be expressed as $d = (x - y) \cdot b + y \cdot a$

This concludes the induction step.

Now what is left to show is that *any other* divisor of a and b also divides d. Suppose c is such a divisor: $c \mid a$, $c \mid b$.

We can write $k \cdot c = a$ and $e \cdot c = b$

$d = (x - y) \cdot b + y \cdot a = (x - y) \cdot e \cdot c + y \cdot k \cdot c = (e \cdot x - e \cdot y + y \cdot k) \cdot c$

Hence, $c \mid d$.

This completes the proof of the theorem for $a, b \geq 0$.

For the case when a and b are not only positive the proof is analogous applying the above to $|a|$ and $|b|$.

$\blacksquare$

Greatest Common Divisor

Claim: There exists a *unique* $d \in \mathbf{Z}$, for any given a, $b \in \mathbf{Z}$, such that: 1) $d \geq 0$

2) $d \mid a$ and $d \mid b$

3) any $c \in \mathbf{Z}$ for which $c \mid a$ and $c \mid b$ it is true that $c \mid d$.

Proof: from the Common Divisor Theorem, there is d with properties 2) and 3). All that is left to prove is 1) and uniqueness. The proof of 1) is easy since if 2) and 3) hold for particular d, than they also hold for ($-d$).

Uniqueness: assume that there is some other d' for which 1), 2) and 3) hold. Then, from 3), we must have $d \mid d' \Rightarrow d \leq d'$ and

$d' \mid d \Rightarrow d' \leq d$, so we must have $d = d'$. ■

Definition: This d is called *greatest common divisor* of a and b, or $gcd(a, b)$

Relative Primes

Definition: $a, b \in \mathbf{Z}$ and $gcd(a, b) = 1$, then a and b are called *relatively prime*.

Property: If $a \mid (b \cdot c)$ and $d = gcd(a, b) = 1$, then $a \mid c$.

Proof: Let $gcd\,(a, b) = 1 = x \cdot a + y \cdot b$ and multiply both sides by c;

$$c = c \cdot x \cdot a + c \cdot b \cdot y.$$ However,

$a \mid (c \cdot x \cdot a)$ apparently, and

$a \mid y \cdot (b \cdot c)$ by hypothesis.

Then, from linearity, $a \mid (c \cdot x \cdot a + c \cdot b \cdot y) = a \mid c$ ■

Modular Arithmetic

In what follows we assume $m > 0$

Definition: we say that a is equal to b mod m if $m \mid (a - b)$ and we write $a = b \bmod m$

Example: 18 = 4 mod 7 = 25 mod 7

Note: There are only m different integers mod m.

A set of m different integers mod m is $\{ 0, 1, 2, \ldots\ m - 1\}$

Properties:

1. $a = a \bmod m$
2. $a = b \bmod m \Rightarrow b = a \bmod m$
3. $a \bmod m = b \bmod m \Rightarrow a = b \bmod m$
4. $a = b \bmod m$ and $b = c \bmod m \Rightarrow a = c \bmod m$

Claim: if $a = b \bmod m$ and $c = d \bmod m,$ then for any $x, y \in \mathbf{Z}$ we have

i) $(a \cdot x + c \cdot y) = (b \cdot x + d \cdot y) \bmod m$

ii) $a \cdot c = b \cdot d \bmod m$

Proof:

i) $m \mid (a - b)$ and $m \mid (c - d)$ by definition. Then, $m \mid x \cdot (a - b)$ and $m \mid y \cdot (c - d)$. From linearity follows that

$$m \mid [x \cdot (a - b) + y \cdot (c - d)] = m \mid [(x \cdot a + y \cdot c) - (x \cdot b + y \cdot d)]$$

which by the definition of mod above gives the desired result.

ii) $m \mid (a - b)$ and $m \mid (c - d)$ by definition. Then

$$m \mid c \cdot (a - b) \text{ and } m \mid b \cdot (c - d)$$

From linearity $m \mid (a \cdot c - b \cdot c + b \cdot c - b \cdot d) = m \mid (a \cdot c - b \cdot d)$

which by the definition of mod above gives the desired result.

■

Theorem *(Cancellation Law)*:

If $a \cdot c = b \cdot c$ mod m and $d = gcd(c, m)$, then $a = b$ mod (m / d)

Proof: $m \mid (a \cdot c - b \cdot c) \Rightarrow m \mid c \cdot (a - b)$. Then there is a k, s.t.

$k \cdot m = c \cdot (a - b)$, and since $gcd(c, m) = d$, we can divide by d

$k \cdot (m / d) = (c / d) \cdot (a - b)$. This means that

$(m / d) \mid [(c / d) \cdot (a - b)]$.

But $gcd(m / d, c / d) = 1$, so we can apply the Relative Primes property and obtain that $(m / d) \mid (a - b)$, which is the desired result by the definition of mod. ■

Euclid's Algorithm

- Algorithm for finding the $gcd(a, b)$
- **Fact:** for $a, b > 0$ there is a *unique* representation

  $a = q \cdot b + r$ with $q, r \geq 0$, where r is called a *remainder*
- **Claim:** $gcd(a, b) = \text{gcd}(b, r)$

  Proof: Write $a = q \cdot b + r$ or $r = a - b \cdot q$. Let $\text{d} = gcd\,(a, b)$. Hence, $d \mid a$ and $d \mid b$ and thus $d \mid r$, d is a divisor of r. We need to show that d is also the gcd of r and b.

$d = a \cdot x + b \cdot y = x \cdot (q \cdot b + r) + b \cdot y = (y + q \cdot x) \cdot b + x \cdot r$

so d is the gcd of r and b. ■

Euclid's Algorithm (cont.)

- Euclid's Algorithm – find $gcd(a, b)$

Use: $gcd(a, b) = gcd(b, r_1) = gcd(r_1, r_2) = \ldots$

$a = q_1 \cdot b + r_1$ $\qquad r_1 = a - q_1 \cdot b$

$b = q_2 \cdot r_1 + r_2$ $\qquad r_2 = b - q_2 \cdot r_1 = -q_2 \cdot a + (q_1 \cdot q_2 + 1) \cdot b$

$r_1 = q_3 \cdot r_2 + r_3$

… $\qquad$ …..

$r_n = q_{n+2} \cdot r_{n-1} + 0$ $\qquad r_{\mathrm{n}-1} = (\ldots) \cdot a + (\ldots) \cdot b$

$\boxed{r_{n-1} = gcd(a, b)}$

these allow us to find *multiplicative inverses*. If some $r_i = 1$, then $1 = \alpha \cdot a + \beta \cdot b$; i.e., a and b are relatively prime. Then $\beta \cdot b = 1 \bmod a$, and β is the inverse of b mod a and α is the inverse of a mod b.

Euclid's Algorithm (cont.)

Example: $a = 5, b = 7$

gcd:	*multiplicative inverses*
$7 = 1 \cdot 5 + 2$	$2 = 7 - 1 \cdot 5$
$5 = 2 \cdot 2 + 1$	$1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (7 - 5)$
$2 = 2 \cdot 1 + 0$	$= -2 \cdot 7 + 3 \cdot 5$
$gcd(5, 7) = 1$	The inverse of 5 mod 7 is 3:
	$3 \cdot 5 = 15 = 1 \bmod 7$
	The inverse of 7 mod 5 is -2,
	$-2 = 3 \bmod 5$
	$7 \cdot 3 = 21 = 1 \bmod 5$

$\mathbf{Z^*_n}$

Definition: Let $\mathbf{Z_n}$ denote the set of integers mod n, namely

$$\mathbf{Z_n} = \{0, 1, 2 \ldots n\text{-}1\}$$

Definition: $\mathbf{Z_n}$* is the set of integers in $\mathbf{Z_n}$ that are relatively prime to n.

Example: $\mathbf{Z_8} = \{0, 1, 2, 3, 4, 5, 6, 7\}$ and $\mathbf{Z_8}^* = \{1, 3, 5, 7\}$

$\mathbf{Z_5} = \{0, 1, 2, 3, 4\}$ and $\mathbf{Z_5}^* = \{1, 2, 3, 4\}$

Claim: $\mathbf{Z_n}^*$ is closed under multiplication mod n. That is,

if $a, b \in \mathbf{Z_n}^*$, then $a \bullet b \in \mathbf{Z_n}^*$.

Proof: a and n are relatively prime so $gcd(a, n) = 1$. Hence there exist $x, y \in \mathbf{Z}$ s.t. $1 = x \bullet a + y \bullet n$, similarly $1 = z \bullet b + v \bullet n$. Multiply these equations and obtain

$$1 = (x \bullet z) \bullet a \bullet b + (v \bullet x \bullet a + y \bullet z \bullet b + v \bullet y \bullet n) \bullet n \Rightarrow$$

$$gcd(a \bullet b, n) = 1 \Rightarrow a \bullet b \in \mathbf{Z_n}^*$$

Theorem: Multiplication of $\mathbf{Z_n}^*$ by some $a \in \mathbf{Z_n}^*$ merely rearranges the elements of $\mathbf{Z_n}^*$

Proof: Denote $\mathbf{Z_n}^* = \{z_1, z_2, \ldots, z_k\}$. Form the previous Claim we know that all $a \bullet z_i \in \mathbf{Z_n}^*$. Take $z_i, z_j \in \mathbf{Z_n}^*$ and $z_i \neq z_j$. Suppose $a \bullet z_i = a \bullet z_j$ mod n but from the Cancellation Law we obtain $z_i = z_j$ mod n, which contradicts the assumption, so we must have $a \bullet z_i \neq a \bullet z_j$ mod n. ■

Euler's Totient Function

Definition: Euler's totient function $\varphi(n)$ is equal to the positive integers that are relatively prime to n and less than n.

$\mathbf{Z_8}$* = { 1, 3, 5, 7} $\varphi(8) = 4$

$\mathbf{Z_7}$* = { 1, 2, 3, 4, 5, 6} $\varphi(7) = 6$

Fact: let p be prime then $\varphi(p) = p - 1$

Euler's Totient Function for $n = p \bullet q$

p, q – prime, $n = p \bullet q$

$Z_{pq} = \{ 0, 1, 2 \; \ldots. ((p \bullet q) - 1)\}$, $|Z_{pq}| = p \bullet q$

Let's show the numbers in Z_{pq} not relatively prime to $p \bullet q$:

$p, 2p \; \ldots. (q - 1) \bullet p \;\rightarrow\; (q - 1)$ numbers

$q, 2q \; \ldots \; (p - 1) \bullet q \;\rightarrow\; (p - 1)$ numbers

$0 \;\rightarrow 1$ number

$$\varphi(p \bullet q) = p \bullet q - 1 - (q - 1) - (p - 1)$$
$$= (p - 1) \bullet (q - 1)$$
$$= \varphi(p) \bullet \varphi(q)$$

Euler's Theorem

Euler's Theorem: for all $a \in \mathbf{Z_n}^*$, $a^{\varphi(n)} = 1 \bmod n$

or, for all $a \in \mathbf{Z_n}^*$ and $k \geq 0$, $a^{k \cdot \varphi(n)+1} = a \bmod n$

Proof: Multiply together all elements of $\mathbf{Z_n}^*$: $x = z_1 \cdot z_2 \ldots z_{\varphi(n)}$.
Now multiply all elements of $\mathbf{Z_n}^*$ by a and multiply them together $(a \cdot z_1) \cdot (a \cdot z_2) \ldots (a \cdot z_{\varphi(n)})$. We showed that multiplication of $\mathbf{Z_n}^*$ by one of its elements merely rearranges the elements in $\mathbf{Z_n}^*$ => $(a \cdot z_1) \cdot (a \cdot z_2) \ldots (a \cdot z_{\varphi(n)}) = x = a^{\varphi(n)} \cdot z_1 \cdot z_2 \ldots z_{\varphi(n)} = x \cdot a^{\varphi(n)}$
But $\mathbf{Z_n}^*$ is closed under multiplication, so $x \in \mathbf{Z_n}^*$. Then x must be relatively prime to n so x has an inverse mod n. Hence, we can multiply both sides of the equation $x = x \cdot a^{\varphi(n)}$ by x^{-1} and obtain $a^{\varphi(n)} = 1 \bmod n$.
Using the above result, it is easy to show that

$$a^{k \cdot \varphi(n)+1} = a^{k.\varphi(n)} \cdot a = 1^k \cdot a = a \bmod n \qquad \blacksquare$$

Generalization of Euler's Theorem

Theorem: If p, q are primes, $n = p \cdot q$,

for all $a \in \mathbf{Z_n}$, $a^{k\cdot\varphi(n)+1} = a \bmod n$.

Proof:

i) If $gcd\ (a, n) = 1$, then this follows from (variant of) Euler's Thm.

ii) If $gcd\ (a, n) \neq 1$, then a, $0 < \text{a} < \text{n} = p \cdot q$, must be a multiple of p or q.

Suppose, wlog, $a = c \cdot p$, where c is a positive integer. In this case, $gcd\ (a, q) = gcd\ (c \cdot p, q) \neq 1$. [Otherwise, since q is prime, c would have to be a multiple of q, which would contradict our hypothesis since $a = r \cdot q \cdot p \geq n$, where r is a positive integer.]

Proof (cont.)

Since $gcd\,(a, q) \neq 1$, by Euler's Theorem, we have

$a^{\varphi(q)} = 1 \bmod q$, and hence by definition of mod. arithm.,
$[a^{\varphi(q)}]^{\varphi(p)} = 1 \bmod q$, and $a^{\varphi(n)} = 1 \bmod q$, which means that
$q \mid a^{\varphi(n)} - 1$, or, for some positive integer k, $a^{\varphi(n)} = 1 + k \bullet q$.

Multiplying both sides of $a^{\varphi(n)} = 1 + k \bullet q$ by $a = c \bullet p$, we obtain
$a^{\varphi(n)+1} = a + k \bullet c \bullet p \bullet q = a + k \bullet c \bullet n = a \bmod n$, and thus
$a^{\varphi(n)} = 1 \bmod n$.

By similar reasoning, we obtain the same result in the case when m is a multiple of q.

But,

$[a^{\varphi(n)}]^{k} = 1^{k} \bmod n$, and

$a^{k \bullet \varphi(n)+1} = a^{k \bullet (p-1)(q-1)+1} = \text{a} \bmod n$. ■

Proof (cont.)

Alternate Proof:

i) If a is relatively prime to n then trivial by variation of Euler's Theorem.

ii) If a is not relatively prime to n, so it must be a multiple of p or q.

Let $a = k \cdot q$ wlog.

$a = k \cdot q = 0 \bmod q$, so $a^{k \cdot \varphi(n)+1} = 0^{k \cdot \varphi(n)+1} \bmod q = a \bmod q = a_1$

$a = a \bmod p$, since $gcd(p, q) = 1$

From Euler's Theorem $a^{\varphi(p)} = 1 \bmod p$, then

$a^{k \cdot \varphi(n)+1} = a^{k \cdot \varphi(p) \cdot \varphi(q)+1} = a \cdot 1^{k \cdot \varphi(q)} = \mathrm{a} \bmod \mathrm{p} = \mathrm{a}_2.$

From *Chinese Remainder Thm.*, $a^{k \cdot \varphi(n)+1} = a_2 \cdot u \cdot p + a_1 v \cdot q \bmod p \cdot q$, where $u \cdot p + v \cdot q = 1$. Substituting the values for $a^{k \cdot \varphi(n)+1} \bmod p$ and $a^{k \cdot \varphi(n)+1} \bmod q$ we get

$a^{k \cdot \varphi(n)+1} = a \cdot u \cdot p + a \cdot v \cdot q = a \cdot (u \cdot p + v \cdot q) = a \bmod p \cdot q$ ■

Chinese Remainder Theorem

Theorem: Let z_1, z_2 and z_N be pairwise relatively prime numbers. If we know that a number is equal to x_1 mod z_1, x_2 mod z_2 … x_N mod z_N , then we can find what the number is

$x \bmod z_1 \cdot z_2 \ldots. z_N$

Proof: $N = 2$, so $x = x_1 \bmod z_1$ and $x = x_2 \bmod z_2$ where $gcd(z_1, z_2) = 1$. Also there exist integers k_1 ,k_2 s.t. $x = x_1+z_1k_1$ and $x = x_2+z_2k_2$. Since $gcd(z_1, z_2) = 1$ there are a and b s.t. $a \cdot z_1+b \cdot z_2= 1$. Multiply both sides by x

$$x = x \cdot a \cdot z_1+x \cdot b \cdot z_2= (x_2 + k_2 \cdot z_2) \cdot a \cdot z_1+ (x_1 + k_1 \cdot z_1) \cdot b \cdot z_2=$$

$$= x_2 \cdot z_1 \cdot a + x_1 \cdot z_2 \cdot b + z_1 \cdot z_2 \cdot (a \cdot k_2 + k_1 \cdot b)$$

Take mod $(z_1 \cdot z_2)$ we obtain:

$$x = (x_2 \cdot z_1 \cdot a + x_1 \cdot z_2 \cdot b) \bmod (z_1 \cdot z_2)$$

Chinese Remainder Thm. (cont.)

Example: $z_1 = 5$, $z_2 = 8$,

$1 = 2 \cdot z_2 - 3 \cdot z_1 \Rightarrow b = 2,\ a = -3$

Number = 3 mod 5 = 2 mod 8

$x_1 = 3$ and $x_2 = 2$, $z_1 \cdot z_2 = 40$

$(x_2 \cdot z_1 \cdot a + x_1 \cdot z_2 \cdot b) = 2 \cdot 5 \cdot (-3) + 3 \cdot 8 \cdot 2 = 18 \bmod 40$

To go the opposite way:

18 = 3 mod 5

18 = 2 mod 8

RSA Block Encryption and Signatures

1. Choose 2 large primes p and q
2. Compute $n = p \cdot q$ and $\varphi(n) = (p - 1) \cdot (q - 1)$
3. Choose *public* e such that $gcd(e, \varphi(n)) = 1$, relatively prime
4. Find *secret* d s.t. $e \cdot d = 1 \bmod \varphi(n)$ (by Euclid's Algorithm)
5. To *encrypt* plaintext block $m < n$, compute the ciphertext $CT = m^e \bmod n$
6. To *decrypt* ciphertext block CT and obtain the plaintext PT

   $PT = CT^d \bmod n = m^{ed} \bmod n$,

   $e \cdot d = 1 \bmod \varphi(n) \Rightarrow e \cdot d = 1 + k \cdot \varphi(n)$

   $PT = m^{k \cdot \varphi(n)+1} \bmod n = m \bmod n$ from Generalized Euler's Theorem.

1. To *sign* plaintext block $m < n$, compute the signature $S = m^d \bmod n$
2. To *verify* that block S is block m's signature, compute $S^e \bmod n = m^{ed} \bmod n$ $= m^{k \cdot \varphi(n)+1} \bmod n = m \bmod n = m$.

Choosing p and q

Preliminary Remarks

1. *Fermat's Theorem* (p = prime, $0 < a < p$) ==> $a^{p-1} = 1 \bmod p$

   <=/=

   holds only in one direction.

   Example: p = 100 digits, $a^{p-1} = 1 \bmod p$, Pr [p =/= prime] ❁ 10^{-13}

2. For same p try multiple values of a to lower Pr [p =/= prime]

   $a_1^{p-1} = 1 \bmod p$, $a_2^{p-1} = 1 \bmod p$, …, $a_n^{p-1} = 1 \bmod p$

   Problem (Carmichael Numbers): there exist values p such that p =/= prime and $a^{p-1} = 1 \bmod p$ for *all* choices of $0 < a < p$.

Primality tests

Recall *Fermat's theorem*: if p is prime, then $a^{p-1} = 1 \bmod p$.

Hence, if p = odd, prime (i.e., not 2), then $p - 1 =$ even, and we can write $(a^{(p-1)/2})^2 = 1 \bmod p$ or $x^2 = 1 \bmod p$, where $x = a^{(p-1)/2}$.

Theorem: If p = odd prime, then $x^2 = 1 \bmod p$ has only two solutions, namely $x = 1$ and $x = -1$.

Proof: $x^2 = 1 \bmod p \Rightarrow x^2 - 1 = 0 \bmod p$

$\Rightarrow (x - 1) \bullet (x + 1) = 0 \bmod p$

$\Rightarrow p \mid (x - 1)$ or $p \mid (x + 1)$ or p divides both.

Suppose p divides both. Hence, $(x + 1) = k \bullet p$ and $(x - 1) = j \bullet p$

Proof of Theorem (ctnd.)

Subtract these two expressions and get:

$(x + 1) - (x - 1) = 2 = (k - j) \bullet p$, which holds only for $p = 2$.

But since p = odd, prime (i.e., different from 2) we reach a contradiction. Hence, $p \mid (x - 1)$ or $p \mid (x + 1)$ but *not* both.

Suppose $p \mid (x - 1)$. Then $(x - 1) = j \bullet p$ for some j.
Thus, $x = 1 \bmod p$ and similarly for $x = -1 \bmod p$.

Stating the Theorem in the opposite direction:

Theorem: If there exists a solution to $x^2 = 1 \bmod p$ other than ± 1, then p is *not* prime.

Examples

- $x^2 = 1 \bmod 7$

  $1^2 = 1 \bmod 7$

  $6^2 = 36 \bmod 7 = 1 \bmod 7$; $6 = -1 \bmod 7$

  Solutions = 1, -1

- $x^2 = 1 \bmod 8$

  $1^2 = 1 \bmod 8$;

  $3^2 = 9 \bmod 8 = 1 \bmod 8$; $3 = -5 \bmod 8$

  $5^2 = 25 \bmod 8 = 1 \bmod 8$; $5 = -3 \bmod 8$

  $7^2 = 49 \bmod 8 = 1 \bmod 8$; $7 = -1 \bmod 8$

  Solutions: 1, -1, 3, -3

Miller-Rabin Test

Part 1: *Quick reject*

Fermat's Theorem: $a^{p-1} = 1 \bmod p$, or $a^{p-1} \bmod p = 1$, if p = prime.

Hence, compute $d = a^{p-1} \bmod p$. If $d \neq 1$, then $d \neq$ prime.

Part 2:

Otherwise, if $d = 1$, there is a possibility that p = prime. Now, we use the result of previous Theorem. That is, at every step of computation of $a^{p-1} \bmod p$ *check* $x^2 = 1 \bmod p$ for roots *other than* ± 1. When computing $d = a^{p-1} \bmod p$, represent $p - 1 = c \cdot 2^b$, where c is odd and $b \neq 0$,

$$a^{p-1} \bmod p = \underbrace{[\ldots[a^c \bmod p]^2 \ldots]^2}_{b \text{ times}}$$

Miller-Rabin Test (cont.)

If early in squaring a^c mod $p \neq 1$, then one squaring took a number $\neq 1$ and squared it to produce 1. However, that number is a square root of 1 mod p. Hence, by the Theorem above $p \neq$ prime.

[If test shows $p \neq$ prime, then more than ¾ of all different values of a will produce p to be composite.]

If the test for p using a single a shows p to be prime, repeat test for other distinct values of a.

- choose s random values of a and repeat the test

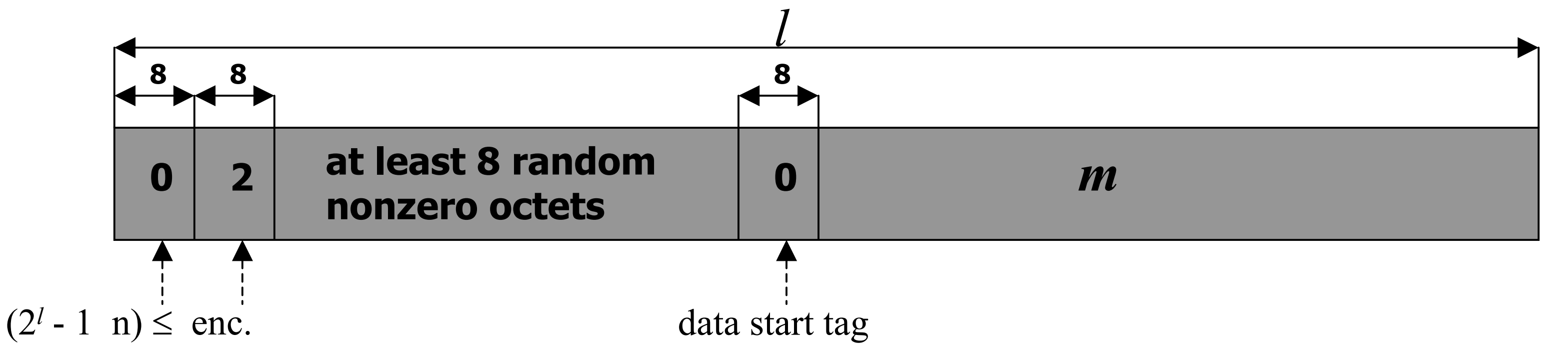
Pr [p = prime] > $1 - 2^{-s}$ or Pr [p =/= prime] $\leq 2^{-s}$.

II. Modes of Encryption for RSA

1. Only short messages should be encrypted

- short message of m bits s.t. $2^l - 1 \leq n$ (RSA modulus)
- performance is one/two orders of magnitude lower than symmetric enc.
- encrypt (probabilistically) long message with symmetric key and encrypt symmetric key (and per message random value) with RSA

2. Example 1: RSA PKCS #1

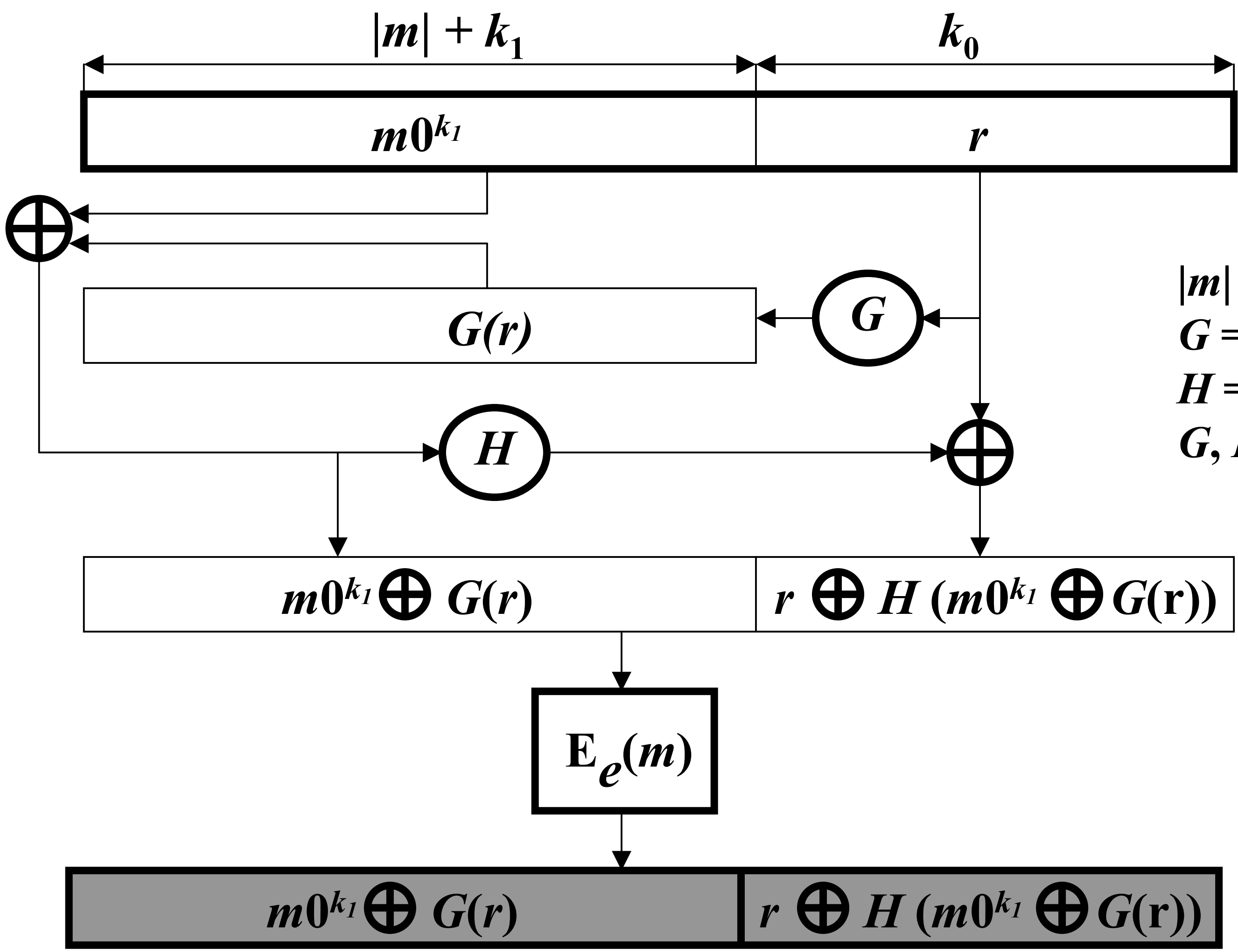


Attack against SSL implementation of PKCS #1based on server (decryption oracle)

- checks the first two bytes and returns errors if malformed
- checks data length and returns errors
- modify ciphertext of encrypted key and in about 2^{20} tries get valid key

II. Modes of Encryption for RSA (ctnd.)

3. Example 2: PKCS #1 version 2 (OAEP-RSA)



$|m| = l - k_0 - k_1$
G **=** generator function
H = hash function
G*, *H **=** random functions

III. Digital Signature for RSA

Example : RSA PKCS #1 Signature for message *m*