RSA Cryptosystem

Ahto Buldas Aleksandr Lenin

March 20, 2020

RSA cryptosystem

In 1977, Ronald Rivest, Adi Shamir and Leonard Adleman proposed the following trapdoor cryptosystem:

- *Private key*: Two large random prime numbers p and q
- *Public key*: Modulus $n = p \cdot q$

Let $e, d \in \mathbb{Z}_{\varphi(n)}$ such that $e \cdot d \equiv 1 \pmod{\varphi(n)}$, where $\varphi(n) = (p-1)(q-1)$ is the Euler's function

- *Encryption* $y = \mathsf{E}_{n,e}(x) = x^e \mod n$
- *Decryption* $\mathsf{D}_{n,d}(y) = y^d \mod n = x$

Questions

- Are E and D efficiently computable?
- Why does the decryption identity $\mathsf{D}_{n,d}(\mathsf{E}_{n,e}(x)) = x$ hold?
- How to find large random prime numbers?

Efficient Exponentiation: Square and Multiply

For efficiently computing $x^e \mod n$ we use the binary expansion:

$$e = e_m \cdot 2^m + e_{m-1} \cdot 2^{m-1} + \ldots + e_1 \cdot 2^1 + e_0 \cdot 2^0 \ ,$$

where $e_m, \ldots, e_0 \in \{0, 1\}$. We use the following computational scheme:

$$\begin{aligned} x^{e_m \cdot 2^m + \ldots + e_0 \cdot 2^0} &= x^{e_m \cdot 2^m} \cdot x^{e_{m-1} \cdot 2^{m-1}} \cdot \ldots \cdot x^{e_0 \cdot 2^0} \\ &= \left(x^{2^m}\right)^{e_m} \cdot \left(x^{2^{m-1}}\right)^{e_{m-1}} \cdot \ldots \cdot \left(x^{2^0}\right)^{e_0} \ . \end{aligned}$$

where the hyper-powers $x^{2^0}, \ldots, x^{2^m}$ are computed by using repeated squaring

$$x^{2^k} = \left(x^{2^{k-1}}\right)^2$$

Euler's Theorem and Decryption Identity

Theorem (Euler)

If $\gcd(x, n) = 1$, *then* $x^{\varphi(n)} \equiv 1 \pmod{n}$.

- We use general group theory to prove Euler's theorem
- By Euler's theorem, if x is invertible modulo n then

$$(x^e)^d = x^{e \cdot d} = x^{1+k\cdot\varphi(n)} = x \cdot \left(x^{\varphi(n)}\right)^k \equiv x \cdot 1^k \equiv x \pmod{n} \ .$$

which means that the *decryption identity* of RSA holds for invertible x.

- Later, we show that decryption identity also holds for non-invertible x

Exercise: Show that finding a non-invertible x modulo $n = pq$ is equivalent to factoring n.

Groups

Group consists of a set G and a binary operation $\cdot$ which is:

- *Associative*: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- *With a unit*: There is $e \in G$ such that $x \cdot e = e \cdot x = x$ for every $x \in G$
- *Invertible*: Every $a \in G$ has an inverse $a^{-1} \in G$, such that $a \cdot a^{-1} = e$

Examples:

- $(\mathbb{Z}, +)$
- $(\mathbb{Z}_n, +)$, where $+$ denotes addition modulo n
- $(\mathbb{Z}_n^*, \cdot)$, where $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \colon \gcd(a, n) = 1\}$ and $\cdot$ is multiplication modulo n

Subgroups

A subset $H \subseteq G$ of a group $(G, \cdot)$ is a *subgroup* if $(H, \cdot)$ is a group.

For example, the set $2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$ of even numbers is a subgroup of the additive group $(\mathbb{Z}, +)$ of integers.

Exercise: Show that for $H \subseteq G$ being a subgroup of $(G, \cdot)$ it is necessary and sufficient that H is closed under multiplication and inverses.

Exercise: Show that for $H \subseteq G$ being a subgroup of *finite* $(G, \cdot)$ it is necessary and sufficient that H is closed under multiplication.

Not true for infinite groups: Although the subset $\mathbb{N} = \{0, 1, 2, \ldots\}$ of $\mathbb{Z}$ is closed under addition, $\mathbb{N}$ is not a subgroup of $(\mathbb{Z}, +)$.

Order of an Element of a Finite Group

Theorem (Order)

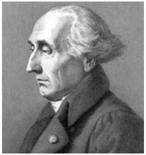
For any element $g \in G$ of a finite group G there exists $n \in \mathbb{N}$ such that $g^n = e$ and $g, g^2, g^3, \ldots, g^n$ are all different. Such n is called the order of g in G and is denoted by $\mathrm{ord}(g)$.

Proof.

As G is finite there is $n \in \mathbb{N}$ such that $g^{n+1} \in \{g, g^2, g^3, \ldots, g^n\}$. Let n be the smallest such number, which also means that $g, g^2, g^3, \ldots, g^n$ are all different. Hence, $g^{n+1} = g$ (and $g^n = e$), because if $g^{n+1} = g^{1+k}$ for $0 < k < n$, then $g^n = g^k \in \{g, g^2, g^3, \ldots, g^{n-1}\}$, contradicting the minimality of n. □

The set $\{g, g^2, g^3, \ldots, g^n\}$ is a subgroup denoted by $\langle g \rangle$ and called the *subgroup generated by g*. Note that $|\langle g \rangle| = \mathrm{ord}(g)$ and $g^{\mathrm{ord}(g)} = e$.

Lagrange's Theorem



Theorem (Lagrange)

If H is a subgroup of a finite group G, then $\frac{|G|}{|H|}$ is an integer.

Proof.

Let $H = \{h_1, \ldots, h_m\}$. For any $g \in G$, let $gH = \{gh_1, \ldots, gh_m\}$, which is called the *co-set* of g. As H has the unit, $g \in gH$ and hence every $g \in G$ is in a co-set. Note that $eH = H$ and hence H is itself a co-set.

If $gh_i = gh_j$, then $h_i = h_j$ and hence all cosets are of equal size $|gH|{=}|H|$.

If $gH \cap g'H \neq \emptyset$, then we have $gH = g'H$. Indeed, if $gh_i = a = g'h_j$, then for every k, we have $gh_k = gh_ih_i^{-1}h_k = ah_i^{-1}h_k = g'h_jh_i^{-1}h_k \in g'H$ and hence $gH \subseteq g'H$, which due to $|gH|{=}|g'H|$ implies $gH = g'H$. Therefore, co-sets split G into a finite number of pieces of size $|H|$. □

Exponentiation Theorem and Proof of Euler's Theorem

Theorem (Exponentiation)

If G is a finite group and $g \in G$, then $g^{|G|} = e$.

Proof.

From Lagrange's theorem, it follows that $\frac{|G|}{|\langle g \rangle|} = k \in \mathbb{N}$ and hence
$g^{|G|} = g^{|\langle g \rangle| \cdot k} = \left(g^{|\langle g \rangle|}\right)^k = 1^k = e$. □

Corollary (Euler's Theorem)

If $\gcd(x, n) = 1$, then $x^{\varphi(n)} \bmod n = 1$

Proof.

The set $\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n \colon \gcd(x, n) = 1\}$ is a group with size $\varphi(n)$. □

Fermat's Theorem and Primality Test

Corollary (Fermat's Theorem)

If p is prime and $0 < x < p$, then $x^{p-1} \equiv 1 \pmod{p}$.

Fermat's primality test (Is n prime?): Pick random $x \leftarrow \{1, \ldots, n-1\}$ and compute $c = x^{n-1} \mod n$.

- If $c \neq 1$, then by Fermat's theorem, n is not prime
- If $c = 1$, then repeat the test
- If test is repeated k times, we stop and claim that n is prime

Question: How reliable is Fermat's test?

Pseudo-Primes to Base b

If n is composite and $b^{n-1} \equiv 1 \pmod{n}$, then n is said to be *pseudo-prime to base b*.

Let $H_n = \{b\colon\ b \in \mathbb{Z}_n^*,\ b^{n-1} \equiv 1 \pmod{n}\}$, i.e. H_n is the set of all invertible bases in $\mathbb{Z}_n$-s, to which n is pseudo-prime.

Theorem

H_n is a subgroup of the multiplicative group $\mathbb{Z}_n^*$.

Proof.

- If $a, b \in H_n$, then $(ab)^{n-1} \equiv a^{n-1} \cdot b^{n-1} \equiv 1 \pmod{n}$. Hence, $ab \in H_n$.
- $1 \in H_n$, because $1^{n-1} = 1$.
- If $a \in H_n$ and $ab \equiv 1 \pmod{n}$, then

$b^{n-1} \equiv a^{n-1} \cdot b^{n-1} \equiv (ab)^{n-1} \equiv 1^{n-1} \equiv 1 \pmod{n}$. □

Carmichael Numbers and the Reliability of Fermat' Test

Definition (Carmichael number)

any composite n with $H_n = \mathbb{Z}_n^*$. The smallest Carmichael number is 561.

Theorem

If n is composite but not a Carmichael number, then $|H_n| \leq \frac{|\mathbb{Z}_n^*|}{2} = \frac{\varphi(n)}{2}$.

Proof.

From $H_n \neq \mathbb{Z}_n^*$ and Lagrange's thm.: $1 < \frac{|\mathbb{Z}_n^*|}{|H_n|} \in \mathbb{N}$. Thus, $\frac{|\mathbb{Z}_n^*|}{|H_n|} \geq 2$. □

Corollary: For composite but not Carmichael numbers the Fermat's test fails with probability $\leq \frac{1}{2}$ and the k-time test with probability $\leq \frac{1}{2^k}$.

How many Carmichael numbers are there?

Theorem (Alford, Granville, Pomerance; 1994)

Let $C(n)$ *be the number of Carmichael numbers in the range* $[0...n]$. *Then* $C(n) > n^{2/7}$. *Hence, there are infinitely many Carmichael numbers.*

Corollary: Fermat's test is not completely trustworthy even for big numbers.

Miller-Rabin's test

- Choose a random $a \leftarrow \{1, \ldots, n-1\}$.
- If $\gcd(a, n) \neq 1$, then output *composite*.
- Let $n - 1 = 2^k \cdot m$, where m is odd.
- If $a^m \mod n = 1$ then output *prime*.
- If $a^{m \cdot 2^i} \equiv -1 \pmod{n}$ for an $i = 0 \ldots k-1$, then output *prime*.
- Otherwise, output *composite*.

Theorem

If n is prime, then Miller-Rabin's test outputs prime.
If n is composite, then the test outputs composite with probability $\geq \frac{1}{2}$.

Chinese Remainder Theorem

Theorem (Chinese Remainder Theorem)

If $\gcd(p,q)=1$ *then the rings* $\mathbb{Z}_{pq}$ *and* $\mathbb{Z}_p\times\mathbb{Z}_q$ *are isomorphic.*

Proof.

Define $f\colon \mathbb{Z}_{pq}\to\mathbb{Z}_p\times\mathbb{Z}_q$ so that $f(x)=(x \bmod p, x \bmod q)$. Obviously, f preserves the ring operations. As $|\mathbb{Z}_{pq}|=|\mathbb{Z}_p\times\mathbb{Z}_q|$, it remains to show that f is injective. For that, we define a mapping $g\colon \mathbb{Z}_p\times\mathbb{Z}_q\to\mathbb{Z}_{pq}$ so that $g(u,v)=(\alpha pv+\beta qu) \bmod pq$, where $\alpha,\beta\in\mathbb{Z}$ and $\alpha p+\beta q=1$. Therefore, if $x\in\mathbb{Z}_{pq}$, $x \bmod p=x-kp$, and $x \bmod q=x-\ell q$, then

$$\begin{aligned} g(f(x)) &= g(x-kp,x-\ell q)=(\alpha p(x-\ell q)+\beta q(x-kp)) \bmod pq \\ &= (\alpha px+\beta qx-pq(\alpha\ell+\beta k)) \bmod pq \\ &= (\alpha px+\beta qx) \bmod pq = x(\alpha p+\beta q) \bmod pq = x\ . \end{aligned}$$

□

Corollary 1: RSA Decryption Identity

Theorem (RSA decryption identity)

If $e \cdot d \equiv 1 \pmod{\varphi(pq)}$, *where* $p \neq q$ *are primes, then for every* $x \in \mathbb{Z}_{pq}$*:*

$$x^{ed} \equiv x \pmod{pq} \ .$$

Proof.

As : $\mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q$, it suffices to prove $(u,v)^{ed} = (u,v)$ in $\mathbb{Z}_p \times \mathbb{Z}_q$. As $(0,0)^{ed} = (0,0)$, we may assume $u, v > 0$. Hence, by Fermat's theorem:

$$\begin{aligned} (u,v)^{ed} &= (u^{ed} \bmod p, v^{ed} \bmod q) = (u^{1+k\varphi(pq)} \bmod p, v^{1+k\varphi(pq)} \bmod q) \\ &= (u \cdot \underbrace{[u^{k(q-1)}]^{p-1} \mod p}_{=1}, v \cdot \underbrace{[v^{k(p-1)}]^{q-1} \mod q}_{=1}) \\ &= (u,v) \end{aligned}$$

□

Corollary 2: Solving Equations

If $\gcd(p, q) = 1$, then for every $u \in \mathbb{Z}_p$ and $v \in \mathbb{Z}_q$ the system

$$\begin{cases} x \mod p = u \\ x \mod q = v \end{cases}$$

has one and only one solution in the interval $[0, 1, 2, ..., pq - 2, pq - 1]$.

Example. Find all solutions x in the interval $[0...20]$:

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 6 \pmod 7. \end{cases}$$

Solution. As $(-2) \cdot 3 + 1 \cdot 7 = 1$, from the proof of Chinese Remainder theorem, it follows that $x \equiv 7 \cdot 2 + (-2) \cdot 3 \cdot 6 \equiv 20 \pmod{21}$, which implies that $x = 20$ is the only solution in $[0...20]$.

Corollary 3: Square Roots of 1

Theorem

If p, q are primes such that $3 \leq p < q$, then the unit $1 \in \mathbb{Z}_{pq}$ has exactly 4 different square roots.

Proof.

It is sufficient to show that the equation $(u, v)^2 = (1, 1)$ has four solutions $(u, v) \in \mathbb{Z}_p \times \mathbb{Z}_q$. This equation is equivalent to the next pair of equations: $u^2 \bmod p = 1$ and $v^2 \bmod q = 1$. Both have exactly two solutions. Indeed, the first equation is equivalent to $(u-1)(u+1) \bmod p = 0$, which implies either $p \mid u - 1$ or $p \mid u + 1$. In the first case $u - 1 = kp$, which means $u = 1$, and in the second case, $u + 1 = kp$ which means $u = p - 1$. As $p > 2$, we never have $1 = p - 1$ and hence these two solutions are different. As both equations have two independent solutions, there are 4 combinations of the solutions everyone being a solution of $(u, v)^2 = 1$. $\square$

Properties of Carmichael Numbers

Theorem

Carmichael numbers are odd.

Proof.

Let n be an even Carmichael number. As n is composite, we conclude that $n \geq 4$. Clearly $n-1 \in \mathbb{Z}_n^*$ but

$$(n-1)^{n-1} = \underbrace{(-1)^{n-1}}_{=-1} + \underbrace{\binom{n-1}{1} n (-1)^{n-2} + \ldots + \binom{n-1}{n-1} n^{n-1} (-1)^0}_{\equiv 0 \pmod{n}}$$

Hence, $(n-1)^{n-1} \bmod n = (-1)^{n-1} \bmod n = n-1 \neq 1$, because $n-1$ is odd and $n-1 \geq 3$. A contradiction. □

Properties of Carmichael Numbers

Theorem

Carmichael numbers are square-free (not divisible by p^2 for any prime p).

Proof.

Let $n = p^k m$ (where $k \geq 2$) be a Carmichael number, where p does not divide m. If $m = 1$, let $b = p + 1$. If $m \geq 3$, let $b \in \mathbb{Z}_n$ be such that

$$\begin{aligned} b &\equiv 1 + p \pmod{p^2} \quad (1) \\ b &\equiv 1 \pmod{m} \quad (2) \end{aligned}$$

In both cases $p^2 \mid b - (p + 1)$. Thus, p does not divide b. Also, $\gcd(b, m) = 1$ (from (2)). Hence, $\gcd(b, n) = 1$ and $b \in \mathbb{Z}_n^*$. Note that $b^{n-1} \equiv (1 + p)^{n-1} \equiv 1 + (n - 1)p \pmod{p^2}$ and $(n - 1)p$ is not divisible by p^2 (as p does not divide $n - 1 = p^k m - 1$). Thus, $b^{n-1} \bmod p^2 \neq 1$, which (as $k \geq 2$) also implies $b^{n-1} \bmod n = b^{n-1} \bmod p^k m \neq 1$. □

Correctness of the Miller-Rabin's Test

Theorem

If n is prime, then the Miller-Rabin's test outputs prime.

Proof.

If $n-1 = 2^k \cdot m$ and m is odd, then for any $a \in \{1, \ldots, n-1\}$ either

- $a^m \equiv 1 \pmod{n}$ (and the test outputs *prime*), or
- $a^m \not\equiv 1 \pmod{n}$, which by $a^{n-1} \equiv 1 \pmod{n}$ (Fermat's theorem!) implies the existence of $i \in \{1, \ldots, k-1\}$ such that $a^{2^i m} \bmod n \neq 1$ and $a^{2^{i+1} m} \bmod n = 1$. Hence, $a^{2^i m} \equiv -1 \pmod{n}$, because otherwise $b = a^{2^i m} \mod n$ would be a non-trivial $\sqrt{1}$ modulo n, which does not exist if n is prime. Hence, also in the second case, the test outputs *prime*

□

Correctness of the Miller-Rabin's Test

Theorem

If n is composite and not a Carmichael number, then the Miller-Rabin's test outputs composite with probability at least $\frac{1}{2}$.

Proof.

By the properties of Fermat's test, $a^{n-1} \not\equiv 1 \pmod{n}$ for at least a half of possible values of a. For such values of a we have $a^m \not\equiv 1 \pmod{n}$ and $a^{m2^i} \not\equiv -1 \pmod{n}$ for any $0 \leq i < k$ and thereby the Miller-Rabin's test outputs *composite*. □

Correctness of the Miller-Rabin's Test

Theorem

For Carmichael numbers the Miller-Rabin's test answers composite with probability at least $\frac{1}{2}$.

Proof. Let n be a Carmichael number, $n-1=2^k\cdot m$ and m be odd. Let $t=\max\{0\le i<k \mid \exists a\in\mathbb{Z}_n^*\colon a^{2^i m}\equiv -1 \pmod n\}$. There is such a t because $(-1)^{2^0 m}=(-1)^m\equiv -1$. If $t'>t$, there is no $a\in\mathbb{Z}_n^*$ such that $a^{2^{t'} m}\equiv -1 \pmod n$. Let

$$B_t=\{a\in\mathbb{Z}_n^*\colon a^{2^t m}\equiv \pm 1 \pmod n\}\ .$$

This set is not empty because there exists $a\in\mathbb{Z}_n^*$ such that $a^{2^t m}\equiv -1 \pmod n$. If $b\notin B_t$ then for such b, the Miller-Rabin's test outputs *composite* because none of the powers $b^{2^{t+1}m},\ldots,b^{2^k m}$ is $\equiv -1$.

Proof continues ...

Let $p \geq 3$ be the smallest prime such that $p \mid n$. As $p^2 \nmid n$, we have $n = pd$ and $\gcd(p, d) = 1$. Let $a^{2^t m} \equiv -1 \pmod{n}$ and $b \in \mathbb{Z}_n$ be such that

$$\begin{aligned} b &\equiv a \pmod{p} \\ b &\equiv 1 \pmod{d} \ . \end{aligned}$$

As both a and 1 are invertible, then so is $b \in \mathbb{Z}_n^*$. At the same time:

$$\begin{aligned} b^{2^t m} &\equiv a^{2^t m} \equiv -1 \pmod{p} \\ b^{2^t m} &\equiv 1^{2^t m} \equiv +1 \pmod{d} \ . \end{aligned}$$

This implies that $b^{2^t m} \not\equiv \pm 1 \pmod{n}$ and hence $b \notin B_t$. It is easy to verify that B_t is a subgroup of $\mathbb{Z}_n^*$ and hence, by the Lagrange's theorem, $\frac{|B_t|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$. □