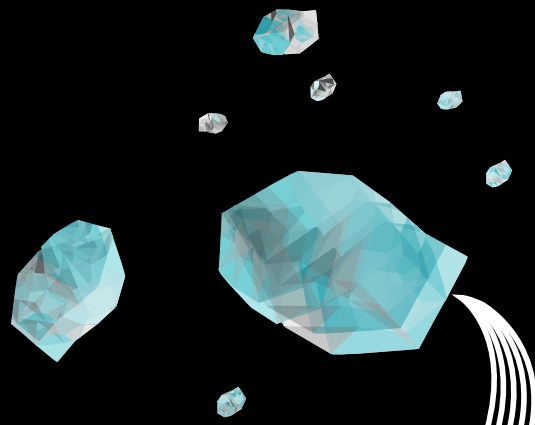
UNIVERSITY OF TWENTE.

Discrete Mathematics 9: The Algorithmic Side of RSA Public Key Encryption

Marc Uetz
m.uetz@utwente.nl



Outline

Reminder: Cyclic Groups

G group, $a \in G$, then

$$< a >= \{a^k \mid k \in \mathbb{Z}\}$$

is the subgroup of G generated by a.

Proposition

If $| < a > |$ finite, then $< a >= \{a, a^2, \ldots, a^{n-1}, a^n\}$ with $a^n = e$ for some $n \in \mathbb{Z}$, and all a^i, $i \in \{1, \ldots, n\}$ are different.

Definition

Group G itself is cyclic if there exists $a \in G$ such that

$$G =< a >$$

More on Cyclic Groups

Question

Given cyclic group $G =< a >$ with $|G| = n$, how many different generators (incuding a) does G have?

Answer. Known as Euler's phi funcion $\phi(n)$
[Exercise 16.2.15 (b) and (c)]

$G = \{a, a^2, \ldots, a^n = e\}$ and part (b) of the exercise says:

$< a^k >= G \Leftrightarrow \gcd(k, n) = 1$

$\phi(n)$ is defined as the number of k's $(1 \leq k < n)$ with $\gcd(k, n) = 1$ (see also Example 8.8 on page 394/395).

Eulers Phi Function

Claim

Let $p_1, \ldots, p_k$ be all prime divisors of n, then

$$\phi(n) = n \prod_{i=1}^{k} (1 - \frac{1}{p_i})$$

Proof

- $\phi(ab) = \phi(a)\phi(b)$ for a, b coprime
- $\phi(p^e) = p^e - p^{e-1} = p^e(1 - \frac{1}{p})$ for p prime
- $\phi(n) = \phi(p_1^{e_1} \cdots p_k^{e_k}) = \prod_{i=1}^{k} p_i^{e_i}(1 - \frac{1}{p_i}) = n \prod_{i=1}^{k} (1 - \frac{1}{p_i})$

□

Notes on $\phi(n)$

Observation

- $\phi(p) = p - 1$ for prime p
- $\phi(pq) = (p-1)(q-1)$ for primes p, q

$G = \mathbb{Z}_n$, and $U_n := \{a \in \mathbb{Z}_n \mid gcd(a, n) = 1\}$ the set of units of $\mathbb{Z}_n$, unitary group

Theorem (also Exercise 16.3.6)

$(U_n, \cdot)$ is a group of order $\phi(n)$ (multiplicative subgroup of $\mathbb{Z}_n$)

Recall: Lagrange Theorem

Theorem 16.9

G finite group, H subgroup, then

$$|H| = m \quad \text{divides} \quad n = |G|$$

Important consequences

G group with $|G| = n$, then

1. for any $a \in G$, $| < a > |$ divides n
2. if $n = p =$ prime, then G is cyclic
3. for any $a \in G$, $a^n = e$ (this is Exercise 16.3.8)

Consequence of Lagrange: Euler's Theorem

Euler's Theorem (Exercise 16.3.13)

Let $n > 1$, $r = \phi(n)$, $M \in \mathbb{Z}$. If $\gcd(M, n) = 1$, then

$$M^r \equiv 1 \pmod{n}$$

Proof. Use consequence 3 of Lagrange theorem □

[Theorem holds even for all $M \in \mathbb{Z}$, not only for $M \in U_n$.
For a proof → Exercise RSA.4]

What is this good for? In RSA, choose n, e and d so that

- encyption: $C \equiv \mathbf{M}^e \pmod{n}$
- decryption: $C^d \equiv M^{ed} \equiv M^{1+kr} \equiv M(M^r)^k \equiv \mathbf{M} \pmod{n}$

Outline

Public key encryption RSA

Rivest, Shamir, Adleman, 1977 (picture from 2003)

Historical note: British Clifford Cocks had equivalent ideas in 1973, documents were declassified only 1997

RSA in Brief

B(ob) wants to send A(lice) a (credit card) number **M**, **secretly**

blue=public
red=secret

Alice chooses n, e cleverly, and

Bob

computes ciphertext $C \equiv \mathbf{M}^e \pmod{n}$

Alice

computes message $\mathbf{M} \equiv C^{\mathbf{d}} \pmod{n}$

(works only with appropriate number **d**, only known to Alice)

RSA in More Detail

What Alice does (**secret** and public)

- chooses two (large) primes $\mathbf{p}, \mathbf{q}$, $n = p \cdot q$
- computes $\mathbf{r} = |U_n| = \phi(n) = (p-1)(q-1)$ $U_n =$ units in $\mathbb{Z}_n$
- chooses exponent $e < r$ with $\gcd(e, r) = 1$ e is a unit in $\mathbb{Z}_r$
- computes $\mathbf{d} = \mathbf{e}^{-1}$ in $\mathbb{Z}_r$ ($ed \equiv 1 \pmod{r}$, i.e., $ed = 1 + kr$)
- publishes only numbers n and number e

What Bob does to send message **M** (any $M \in \mathbb{Z}_n$ possible)

compute ciphertext $C = \mathbf{M}^e \pmod{n}$, email C to Alice

What Alice does to decrypt message C

compute $C^{\mathbf{d}} \equiv (M^e)^d \equiv M^{ed} \equiv M^{1+kr} \equiv M \cdot (M^r)^k \equiv \mathbf{M} \pmod{n}$

Where Lagrange / Euler Comes In

What Alice does to decrypt message C

compute $C^{\mathbf{d}} \equiv (M^e)^d \equiv M^{ed} \equiv M^{1+kr} \equiv M \cdot (M^r)^k \equiv \mathbf{M} \pmod{n}$

$\uparrow$

$M^r \equiv 1 \pmod{n}$, follows from Euler's Theorem (if $M \in U_n$ already proved, and if $M \in \mathbb{Z}_n \rightarrow$ Exercise RSA.4)

RSA: An example

Alice

- $p = 3$ and $q = 11$, so $n = 33$ and $r = \phi(n) = 2 \cdot 20 = 20$
- choose $e = 7$ relatively prime with 20
- compute $d = 3 = 7^{-1}$ (in $\mathbb{Z}_{20}$)
- publish $n = 33$ and $e = 7$

Bob's credit card number is $M = 8$

Computes $C \equiv M^e \equiv 8^7 \equiv 8(8^2)^3 \equiv 8(-2)^3 \equiv -64 \equiv 2 \pmod{33}$

Alice

Computes $M \equiv C^d \equiv 2^3 \equiv 8 \pmod{33}$

What Alice Needs to Do

- chooses $n = pq$, computes $r = |U_n| = (p-1)(q-1)$ $\surd$
- chooses $e < r$ with $\gcd(e, r) = 1$ (e unit in $\mathbb{Z}_r$)
  e.g., e uniformly at random in $1, \ldots, r-1$, chance to hit unit in $\mathbb{Z}_r$ is $\phi(r)/(r-1)$, so repeat until e unit is found $\surd$
- computes $d = e^{-1}$ in $\mathbb{Z}_r$
  $[d] = [e]^{-1}$, Example 14.13, Extended Euclidean Algorithm: divide r by e to get $1 = d \cdot e - k \cdot r$, so that $[1] = [d] \cdot [e]$ $\surd$
- computes $M = C^d \pmod{n}$
  by modular exponentiation, the algorithm in Example 14.16 $\surd$

- all this can be done **efficiently** (i.e. in polynomial time)

What Bob Needs to Do

Bob...

- computes $C = M^e \pmod{n}$
  by modular exponentiation, the algorithm in Example 14.16 $\surd$

- this can be done **efficiently**, too

Modular Exponentiation

Want to compute efficiently

$$C^d \pmod{n}$$

1) We exploit the fact that

$$ab \pmod{n} = (a \pmod{n}) \cdot (b \pmod{n})$$

2) We write exponent d in binary. Example: $3^{20} \pmod{5}$.
$20 = 2^4 + 2^2 = 10100_2$ (binary). Now compute, in this order:

$$3^{2^0} = 3 \pmod{5}$$
$$3^{2^1} = (3^{2^0})^2 = 3^2 = 4 \pmod{5}$$
$$3^{2^2} = (3^{2^1})^2 = 4^2 = 1 \pmod{5}$$
$$3^{2^3} = (3^{2^2})^2 = 1^2 = 1 \pmod{5}$$
$$3^{2^4} = (3^{2^3})^2 = 1^2 = 1 \pmod{5}$$

$$\text{so we have } 3^{20} = 3^{2^2} 3^{2^4} = 1 \cdot 1 = 1 \pmod{5}$$

Note that we need only $O(\log_2 d)$ multiplications

What Eve (eavesdropper) needs to break the code

What Eve knows

- all public information, n, e, and C

What Eve needs

- Alice's private decryption key, d such that $C^d = M \pmod{n}$

So Eve needs r to compute $d = e^{-1}$ (in $\mathbb{Z}_r$, not in $\mathbb{Z}_n$), but therefore, Eve needs to know p and q, so after all, Eve needs

the **prime factorization of** n (recall, $n = pq$)

so far this **can't be done efficiently** (an open problem!)

For Exam

Make sure that you can do things like

Compute $25^{-1} \pmod{72}$

[Answer: $-23 = 72 - 23 = 49$; extended Euclidean algorithm]

Compute last digit of 9^{421}

[compute $9^{421} \pmod{10}$, by modular exponentiation, or:
$9^{421} = 9(9^{420}) = 9((9^2)^{210}) = 9 \pmod{10}$]

Worked Out Example + More Information

http://en.wikipedia.org/wiki/RSA

Please see pdf on RSA on canvas, incl. tutorial exercises !

Thank you for your attention !