Introduction to cryptology (GBIN8U16)

✧

RSA

Pierre Karpman
pierre.karpman@univ-grenoble-alpes.fr
https://www-ljk.imag.fr/membres/Pierre.Karpman/tea.html

2019–03/04

Back to basics

Greatest common divisor (GCD)

The *greatest common divisor* of two numbers a, $b \in \mathbb{N}$ is the largest number k, noted $\mathrm{gcd}(a, b)$ s.t. $a = km$, $b = km'$ for some m, $m' \in \mathbb{N}$

Co-primality

Two integers a, b are called *coprime* if $\mathrm{gcd}(a, b) = 1$

Examples:

- $\mathrm{gcd}(n, n) = \mathrm{gcd}(n, 0) = n$ for any n
- $\mathrm{gcd}(n, 1) = 1$ for any n
- $\mathrm{gcd}(n, kn) = n$ for any n
- $\mathrm{gcd}(p, q) = 1$ for any two prime numbers p, q
- $\mathrm{gcd}(p, n) = 1$ for any $n < p$

GCD computation

Given two integers, it is:

- Very important to be able to compute their gcd
- Very easy to do so (cool!)

$\rightsquigarrow$

A nice recurrence:

- Let $a, b \in \mathbb{N}$, $a > b$
- Then $k = \gcd(a, b) = \gcd(b, a \mod b)$
  - If $a \mod b = 0$, then $a = kb \Rightarrow \gcd(a, b) = \gcd(b, 0) = b$
  - If $a \mod b = r$, then $a = km = qb + r$, $b = km'$
  - $\Rightarrow km = qkm' + r \Rightarrow k(m - qm') = r \Rightarrow$ k divides r too!

Euclid's algorithm

The previous recurrence leads to Euclid's algorithm for gcd computation

GCD computation (recursive)

Input: a, $b < a$
Output: $\gcd(a, b)$

1. If $b = 0$, return a
2. Return $\gcd(b, a \mod b)$

In practice, iterative versions may be preferable

Extended Euclid

Let a, b, $k = \gcd(a, b)$

- Then for any u, $v \in \mathbb{Z}$,
  $ua + vb = ukm + vkm' = k(um + vm') = kw$ with
  $w = um + vm'$
- Of particular interest are any *Bézout coefficients* u, v s.t.
  $um + vm' = 1$, then we have $ua + vb = k = \gcd(a, b)$
- One can easily compute such u, v by *extending* Euclid's algorithm

Extended Euclid (cont.)

1. Start from the equalities $(1): 1 \times a + 0 \times b = a$; $(2): 0 \times a + 1 \times b = b$
2. Compute the division $a = q \times b + r$, then $(1) - q \times (2) = 1 \times a - q \times b = r$
3. Iterate until r becomes 1 or 0

Example

$\rightsquigarrow$ On the board

Extended Euclid w/ Matrices

- Define $R_0 := b$, $R_1 := a$. The sequence of remainders in Euclid's algorithm is obtained as $\begin{pmatrix} R_{i+1} \\ R_{i+2} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -Q_i \end{pmatrix} \begin{pmatrix} R_i \\ R_{i+1} \end{pmatrix}$
- Define $T_i := \begin{pmatrix} 0 & 1 \\ 1 & -Q_i \end{pmatrix}$, one has $\begin{pmatrix} R_{i+1} \\ R_{i+2} \end{pmatrix} = T_i \dots T_1 T_0 \begin{pmatrix} R_0 \\ R_1 \end{pmatrix}$
- and $\begin{pmatrix} G \\ 0 \end{pmatrix} = T_{k-1} \dots T_1 T_0 \begin{pmatrix} R_0 \\ R_1 \end{pmatrix}$ for some k, where G is the gcd of a and b
- and if one defines $M := T_{k-1} \dots T_1 T_0$, one has $G = M_{0,0} R_0 + M_{0,1} R_1$, $\Rightarrow$ Bézout coefficients from M

Note: Fast gcd algorithms exist to compute M with less work than k iterations

Applications: Dividing in $\mathbb{Z}/N\mathbb{Z}$

Let $a, b \in \mathbb{Z}/N\mathbb{Z}$, one wants to compute a/b

- Assuming we know how to multiply, we just need to compute b^{-1}
- To do this, compute u, v s.t. $ub + vN = 1 = \gcd(b, N)$
  - If $\gcd(b, N) > 1$, b is not invertible $\mod N$ (why?)
- Then $ub = 1 - vN \Rightarrow ub \equiv 1 \mod N \Rightarrow u = b^{-1}$

Exercise: use this algorithm to prove that $\mathbb{Z}/N\mathbb{Z}$ is a field iff N is prime

Digression: Little Fermat Theorem

Another possibility to find the inverse of $a \in \mathbb{Z}/N\mathbb{Z}$ when N is prime is to use the Little Fermat Theorem (LFT)

Little Fermat Theorem

Let p be a prime number, then for any $0 < a < p$, one has $a^{p-1} \equiv 1 \mod p$.

Applications: Chinese Remainder Theorem

The (simple) Chinese Remainder Theorem (CRT)

Let $m_1, \ldots, m_k$ be k pairwise coprime (positive) integers ($\forall i, j \gcd(m_i, m_j) = 1$) and $x_1, \ldots, x_k$ any integers (for simplicity s.t. $0 \leq x_i < m_i$), then there is a unique $x \mod \prod_i m_i$ s.t. $x \equiv x_i \mod m_i$ for all $1 \geq i \geq k$

- Given x, m_i, it is easy to compute $x_i = x \mod m_i$
- The inverse problem is in fact also easy, using the extended Euclid algorithm

Note: This theorem is very useful! (E.g. used in the admitted Pohlig-Hellman algorithm; also nice to speed-up modular/big number arithmetic)

CRT: how?

CRT reconstruction (Lagrange basis)

Input: $m_1, \ldots, m_k, x_1, \ldots, x_k$
Output: The unique $0 \geq x < \prod m_i$ s.t. $x \equiv x_i \mod m_i$

1. Let $M \leftarrow \prod_i m_i$
2. For all $1 \geq i \geq k$
3. $\quad M_i \leftarrow M/m_i$
4. $\quad$ Let a_i be such that $a_i M_i \equiv 1 \mod m_i$ ▷ *Computed from* $\gcd(M_i, m_i) = 1$
5. $\quad$ Let $X_i \leftarrow a_i M_i x_i$ ▷ $X_i \equiv x_i \mod m_i; X_i \equiv 0 \mod m_{j \neq i}$
6. Return $\sum_i X_i \mod M$

Back to Crypto: RSA

RSA (Rivest, Shamir, Adleman, 1977) in a nutshell: a family of "one-way permutations with trapdoor"

- Publicly define $\mathcal{P}$ that everyone can compute
- Knowing $\mathcal{P}$, it is "hard" to compute $\mathcal{P}^{-1}$ (even on a single point)
- There is a *trapdoor* associated w/ $\mathcal{P}$
- Knowing the trapdoor, it is easy to compute $\mathcal{P}^{-1}$ everywhere

RSA: how?

- Let p, q be two (large) prime numbers
- Let $N = pq$
- Any $0 < x < N$ s.t. $\gcd(x, N) = 1$ is invertible in $\mathbb{Z}/N\mathbb{Z}$
  - Note that knowing $x \notin (\mathbb{Z}/N\mathbb{Z})^\times \Leftrightarrow$ knowing p and q
  - Why?

Proposition: order of $(\mathbb{Z}/N\mathbb{Z})^\times$

Let N be as above, the order of the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^\times$ is equal to $(p-1)(q-1)$. (More generally, it is equal to $\varphi(N)$)

- So for any $x \in (\mathbb{Z}/N\mathbb{Z})^\times$, $x^{k\,\varphi(N)+1} = x$

RSA: more on how

- Let e be s.t. $\gcd(e, \varphi(N)) = 1$; consider $\mathcal{P} : x \mapsto x^e \mod N$
- $\mathcal{P}$ is a permutation over $(\mathbb{Z}/N\mathbb{Z})^\times$ (in fact over $\mathbb{Z}/N\mathbb{Z}$)
- Knowing e, N, it is easy to compute $\mathcal{P}$
- Knowing e, $\varphi(N)$, it is easy to compute d s.t. $ed \equiv 1 \mod \varphi(N)$
- Knowing d, x^e, it is easy to compute $x = x^{ed}$

$\Rightarrow$ We have a permutation with trapdoor, but how good is the latter?

RSA: how secure?

Knowing $ed = k\,\varphi(N) + 1$, it is easy to find $\varphi(N)$ (admitted)

Knowing $N = pq$, $\varphi(N) = (p-1)(q-1)$, it is easy to find p and q

- $\varphi(N) = pq - (p+q) + 1$; $p + q = -(\varphi(N) - N - 1)$
- For any a, b, knowing ab and $a + b$ allows to find a and b
  - Consider the polynomial $(X-a)(X-b) = X^2 - (a+b)X + ab$
  - $\Delta = (a+b)^2 - 4ab = (a-b)^2$
  - $a = ((a+b) + (a-b))/2$

$\Rightarrow$ Knowing, N, e, d, it is easy to factor N, plus:

- e does not (really) depend on N

$\Rightarrow$ If it is easy to compute d from N, e, it is easy to factor N, and

- It is a hard problem to factor $N = pq$ when p, q are large random primes

BUT it might not be necessary to know d to (efficiently) invert $\mathcal{P}$

Recap: the RSA permutation family

- Let $N = pq$, with p, q prime numbers
- Let e be s.t. $\gcd(e, \varphi(N) = (p-1)(q-1)) = 1$
  - In practice, e is often fixed to $3 = 2 + 1$ or $65537 = 2^{16} + 1$
- The RSA permutation $\mathcal{P}$ over $\mathbb{Z}/N\mathbb{Z}$ is given by $m \mapsto m^e$
- The inverse $\mathcal{P}^{-1}$ is given by $m \mapsto m^d$, where $ed \equiv 1 \mod \varphi(N)$
- N, e are the *public parameters* defining $\mathcal{P}$
- N, e, d are the *private parameters* defining $\mathcal{P}$, $\mathcal{P}^{-1}$

Assumption: Given only the public parameters, it is “hard” to invert $\mathcal{P}$

RSA for PKC

The objective: use RSA to build

- Public-key (asymmetric) encryption
  - Can then be used for asymmetric key exchange
- Public-key signatures

These schemes will need to satisfy the usual security notions

- For encryption: IND-CPA/CCA (“semantic security”)
- For signatures: Existential unforgeability under chosen-message attacks (EUF-CMA)

IND-CCA for Public-Key encryption

IND-CCA for $(\mathsf{Enc}, \mathsf{Dec})$: An adversary cannot distinguish $\mathsf{Enc}(pk_C, 0)$ from $\mathsf{Enc}(pk_C, 1)$, when given (restricted) oracle access to $\mathsf{Dec}(sk_C, \cdot)$ oracle:

1. The Challenger chooses a key pair (pk_C, sk_C), a random bit b, sends $c = \mathsf{Enc}(pk_C, b)$, pk_C to the Adversary
2. The Adversary may repeatedly submit queries $x_i \neq c$ to the Challenger
3. The Challenger answers a query with $\mathsf{Dec}(sk_C, x_i) \in \{0, 1, \perp\}$
   - This assumes w.l.o.g. that the domain of Enc is $\{0, 1\}$, and that decryption may fail
4. The Adversary tries to guess b

EUF-CMA for Public-Key signatures

EUF-CMA for $(\mathrm{Sig}, \mathrm{Ver})$: An adversary cannot forge a valid signature σ for a message m such that $\mathrm{Ver}(pk_C, \sigma, m)$ succeeds, when given (restricted) oracle access to $\mathrm{Sig}(sk_C, \cdot)$:

1. The Challenger chooses a pair (pk_C, sk_C) and sends pk_C to the Adversary
2. The Adversary may repeatedly submit queries m_i to the Challenger
3. The Challenger answers a query with $\sigma_i = \mathrm{Sig}(sk_C, m_i)$
4. The Adversary tries to forge a signature σ_f for a message $m_f \neq_i m_i$, s.t. $\mathrm{Ver}(pk_C, \sigma_f, m_f) = \top$

RSA Encryption: first attempt

Let $\mathcal{P}, \mathcal{P}^{-1}$ be RSA permutations with parameters N, e, d. Define:

- $\mathrm{Enc}(pk = (N, e), m) = \mathcal{P}(m) = (m^e \mod N)$
- $\mathrm{Dec}(sk = (N, e, d), c) = \mathcal{P}^{-1}(c) = (c^d \mod N)$

Not randomized ⇒ fails miserably, not IND-CCA

- When receiving $c = \mathcal{P}(b)$, the Adversary compares with $c_0 = \mathcal{P}(0)$, $c_1 = \mathcal{P}(1)$

More issues with raw RSA

- If m, e are small, it may be that $m^e \mod N = m^e$ (over the integers) $\Rightarrow$ trivial to invert
  - Example: N is of 2048 bits, $e = 3$, m is a one-bit challenge: adding 512 random bits of padding before encrypting does not provide IND-CCA security!
- Consider a *broadcast* setting where m is encrypted as $c_i = m^3 \mod N_i$, $i \in [\![1, 3]\!]$. Suppose that $\forall i$, $m < N_i < c_i$. Using the CRT, one can reconstruct $m^3 \mod N_1 N_2 N_3 = m^3$ and retrieve m.
  - Even random padding might not prevent this attack, if too structured (Hastad, Coppersmith)

More issues with (semi-)raw RSA

A very useful result for analysing the security of RSA is due to Coppersmith (1996):

Finding small modular roots of univariate polynomials

Let P be a polynomial of degree k defined modulo N, then there is an efficient algorithm that computes its roots that are less than $N^{1/k}$

- The complexity of the algorithm is polynomial in k (but w/ a high degree)
- Example application: if $c = (2^k B + x)^3 \mod N$ is an RSA "ciphertext", B is known and of size $2/3 \log(N)$, one can find x of size $k < 1/3 \log(N)$ by solving $(2^k B + X)^3 - c = 0$
- Other applications: in the previous slide; in slide #28, ...

Proper RSA-ENC

Let $\mathcal{P}, \mathcal{P}^{-1}$ be RSA permutations with parameters N, e, d. Let Pad, Pad^{-1} be a padding function and its inverse. Define:

- $\mathsf{Enc}(pk = (N, e), m) = \mathcal{P}(\mathsf{Pad}(m)) = (\mathsf{Pad}(m)^e \mod N)$
- $\mathsf{Dec}(sk = (N, e, d), c) = \mathsf{Pad}^{-1}(\mathcal{P}^{-1}(c)) = \mathsf{Pad}^{-1}(c^d \mod N)$

Necessary conditions on Pad:

- It must be invertible
- It must be randomized (with a large-enough number of bits)
- For all m, N, e, $\mathsf{Pad}(m)^e$ must be larger than N

OAEP: A good padding function for RSA-ENC

OAEP: Optimal Asymmetric Encryption Padding (Bellare & Rogaway, 1994):

- Let $k = \lfloor \log(N) \rfloor$, κ be a security parameter
- Let $\mathcal{G} : \{0,1\}^\kappa \to \{0,1\}^n$, $\mathcal{H} : \{0,1\}^n \to \{0,1\}^\kappa$ be two hash functions
- Define $\mathrm{Pad}(x)$ as $(y_L \| y_R) = x \oplus \mathcal{G}(r) \| r \oplus \mathcal{H}(x \oplus \mathcal{G}(r))$, where $r \xleftarrow{\$} \{0,1\}^\kappa$
- One has $x = \mathrm{Pad}^{-1}(y_L \| y_R) = y_L \oplus \mathcal{G}(y_R \oplus \mathcal{H}(y_L))$

More on OAEP

- OAEP essentially uses a two-round Feistel structure
- To be instantiated, it requires two hash functions $\mathcal{H}$ and $\mathcal{G}$ with variable output size
- A possibility is to use a single XOF $\mathcal{X} : \{0,1\}^* \rightarrow \{0,1\}^*$, such as SHAKE-128

OAEP: Why does it work (kind of)?

Intuitively, full knowledge of $(y_L || y_R)$ is necessary to invert:

- If part of y_L is unknown, $\mathcal{H}(y_L)$, then $\mathcal{G}(y_R \oplus \mathcal{H}(y_L))$ are uniformly random
- If part of y_R is unknown, $\mathcal{G}(y_R \oplus \mathcal{H}(y_L))$ is uniformly random
- In both cases $\Rightarrow$ x is hidden by a "one-time-pad"

More formally, we would like a reduction of the form:

$$\text{Breaking RSA-OAEP w. Adv. } \epsilon \Rightarrow \text{Inverting RSA w. Adv. } \approx \epsilon$$

Exercise: Why would this give us a useful reduction?

OAEP woes

- The original proof that OWP-OAEP is IND-CCA (for any good OWP) (Bellare & Rogaway, 1994) was incorrect
- Shoup showed that there can be no such proof (2001)
- But when OWP is RSA, then there *is* a proof (Shoup, 2001; Fujisaki & al., 2000)!
  - Exploits Coppersmith's algorithm!
- Not all the proofs are *tight* (e.g. Adv. $\epsilon \Rightarrow$ Adv. ϵ^2)
  - Need large parameters to give a meaningful guarantee

What about RSA-SIG now?

Let $\mathcal{P}, \mathcal{P}^{-1}$ be RSA permutations with parameters N, e, d. Define:

- $\mathrm{Sig}(sk = (N, e, d), m) = \mathcal{P}^{-1}(m)$
- $\mathrm{Ver}(pk = (N, e), \sigma, m) = \mathcal{P}(\sigma) == m \; ? \; \top : \bot$

Why this might work:

- Correctness: $(m^d)^e \equiv m \mod N$ ($\mathcal{P}^{-1} \circ \mathcal{P} = \mathcal{P} \circ \mathcal{P}^{-1} = \mathrm{Id}$)
- Security: Comes from the hardness of inverting $\mathcal{P}$ w/o knowing $d \rightsquigarrow$ forging a signature for $m \Leftarrow$ compute $\mathcal{P}^{-1}(m)$

Raw RSA-SIG: That's no good!

- If $m \equiv m' \mod N$, then $\mathcal{P}^{-1}(m) = \mathcal{P}^{-1}(m) \Rightarrow$ trivial forgeries
- $\mathcal{P}^{-1}(m)\mathcal{P}^{-1}(m') = (m^d)(m'^d) \mod N = (mm')^d \mod N = \mathcal{P}^{-1}(mm') \Rightarrow$ trivial forgeries over $[\![0, N-1]\!]$

Again, some padding is necessary!

Proper RSA-SIG

Let $\mathcal{P}, \mathcal{P}^{-1}$ be RSA permutations with parameters N, e, d. Let Pad be a padding function. Define:

- $\mathsf{Sig}(sk = (N, e, d), m) = \mathcal{P}^{-1}(\mathsf{Pad}(m))$
- $\mathsf{Ver}(pk = (N, e), \sigma, m) = \mathcal{P}(\sigma) == \mathsf{Pad}(m)\ ?\ \top : \bot$

- Pad does not need to be invertible
- It does not need to be randomized (tho this can help)

What padding functions for RSA-SIG?

Let $k = \lfloor \log(N) \rfloor$

Full-Domain Hash (FDH) (Bellare & Rogaway; 1993):

- Let $\mathcal{H} : \{0,1\}^* \rightarrow \{0,1\}^k$ be a hash function, $\mathrm{Pad}(m) = \mathcal{H}(m)$

PFDH (Coron, 2002):

- Let $\mathcal{H} : \{0,1\}^* \rightarrow \{0,1\}^k$ be a hash function, $r \overset{\$}{\leftarrow} \{0,1\}^n$, $\mathrm{Pad}(m) = \mathcal{H}(m \| r)$
  - r is not included in the padding *per se*, but must be transmitted along

- Both are pretty simple, both provable in the random oracle model (ROM)
- The proof is *tighter* for PFDH ("good" security is obtained for smaller N)
- $\mathcal{H}$ can instantiated by a XOF

Another nice padding: PSS-R

PSS-R (Bellare & Rogaway, 1996):

- Let $\lfloor \log(N) \rfloor = k = k_0 + k_1 + k_2$, $\mathcal{H} : \{0,1\}^{k-k_1} \to \{0,1\}^{k_1}$, $\mathcal{G} : \{0,1\}^{k_1} \to \{0,1\}^{k-k_1}$ be two hash functions, $r \xleftarrow{\$} \{0,1\}^{k_0}$
- $\mathsf{Pad} : \{0,1\}^{k_2} \to \{0,1\}^{k}$ is defined by $\mathsf{Pad}(x) = \mathcal{H}(x \| r) \| (x \| r \oplus \mathcal{G}(\mathcal{H}(x \| r)))$
- If $|x| < k_2$, PSS-R is invertible (then, the message m does not need to be transmitted with the signature)
- Otherwise, e.g. compute $\mathsf{Pad}(x')$ where $x' = \mathcal{I}(x)$, $\mathcal{I} : \{0,1\}^{*} \to \{0,1\}^{k_2}$ a hash function (then, k_2 must be "large enough")

More on PSS-R

- In fact, PSS-R may also be used as padding for RSA-ENC (Coron & al., 2002)!
  - Notice the relative similarity between PSS-R and OAEP
- Both SIG and ENC cases are provably secure in the ROM
  - In the specific case of RSA, same as OAEP

RSA-SIG: Quick implementation comments

- The signer knows N, e, d, and also the factorization $p \times q$ of N
- Thanks to the CRT, any computation mod N (in particular $m \mapsto m^d$ may be done mod p and mod q
- A CRT implementation is more efficient, as multiplying two numbers does not have a linear cost
- In fact, such CRT decomposition is a useful approach for general big number arithmetic
- $\Rightarrow$ "RSA-CRT" implementations
  - More efficient, but beware of fault attacks! (That's a general warning, tho)

RSA on the side

One can also use the RSA permutation to define a PRNG (Micali & Schnorr, 1988). Let (N, e) be RSA parameters, $n = \log(N)$, then:

1. Start with a random (secret) seed $x_0 \in [\![0, 2^r[\![$, $2^r \ll N$
2. Step the generator by computing $v_i = x_{i-1}^e \mod N$
3. Extract the next secret state x_i from $v_i = 2^k x_i + w_i$, $k = n - r$
4. Output w_i as pseudo-random bits

Question: how small can r be?

- Should be at least n/e, otherwise modular reduction may not happen
- Micali and Schnorr proposed $2n/e$, which seems okay (Fouque & Zapalowicz, 2014)

RSA, DH recap, comparison

Roughly, hardness of factoring, DLOG $\Rightarrow$ Asymmetric key exchange, public-key signatures

- Factoring $\rightsquigarrow$ RSA: One-way permutation w/ trapdoor, can be used for both
- DLOG $\rightsquigarrow$ DH, Schnorr/DSA/...: No permutation, but same functionalities

There are some differences, tho

Some DLOG schemes properties

- For key exchange, can change the secret every time ⇒ "forward secrecy"
- For (the popular schemes for) signatures, good randomness is essential! (Otherwise it breaks)
- Picking a random exponent is easy
- Picking a good group is not completely staightforward
- Some active attacks are possible
- It is possible to "break entire groups" (e.g. $\mathbb{F}_p^\times$)

Some RSA properties

- Secrets are fixed ⇒ a break can compromise a long history
- No randomness needed for signatures (e.g. basic FDH), randomness failures don't reveal the secret
- Generating parameters is somewhat hard
- But all of them are independent (in principle)