Cryptography & Encryption:6G7Z1011 : The RSA Algorithm

Keith Yates

March 1, 2019

RSA Encryption

Today we discuss the RSA encryption algorithm (it is named after its creators Rivest, Shamir and Adleman), it is the most important and widely used public-key encryption algorithm. When you communicate securely over the internet, for example with bill payments and online shopping, then the algorithm used is RSA (or some small variant).

Theoretical Ideas

The algorithm rests on three theoretical concepts

1. The evaluation of inverses $\mod n$, recall for $x \in \mathbb{Z}$ then its multiplicative inverse $\mod n$ (if it exists) was the y such that $xy = 1 \mod n$.
2. The Euler function $\phi(n)$, recall

$$\phi : \mathbb{N} \to \mathbb{N}, n \mapsto \phi(n) = \left|\{i \mid 1 \leq i \leq n, \gcd(i, n) = 1\}\right|. \tag{0.1}$$

3. Euler's theorem: if a is invertible $\mod n$ then

$$a^{\phi(k)} = 1 \mod k. \tag{0.2}$$

Properties of ϕ

To get you thinking.

$$\phi : \mathbb{N} \to \mathbb{N}, n \mapsto \phi(n) = |\{i \mid 1 \le i \le n, \gcd(i,n) = 1\}| . \tag{0.3}$$

1. What is $\phi(p)$ for p prime?
2. Verify directly $\phi(15) = \phi(3)\phi(5)$
3. Prove $\phi(p^i) = p^{i-1}(p-1)$

Answers

1. $\phi(p) = p - 1$ because for every $1 \leq i < p$ we have $\gcd(i, n) = 1$
2. $\phi(15) = \phi(3)\phi(5)$:
   a) $\phi(3) = |\{1, 2\}| = 2$, $\phi(5) = |\{1, 2, 3, 4\}| = 4$,
   b) $\phi(15) = |1, 2, 4, 7, 8, 11, 13, 14|$ because $\gcd(3, 15) = 3$, $\gcd(5, 15) = 4$ $\gcd(6, 15) = 3$, $\gcd(9, 15) = 3$, $\gcd(10, 15) = 5$, $\gcd(12, 15) = 3$.
3. More of a challenge

Trapdoor Function

Let $f : X \to Y$ denote any function, with no loss of generality we assume the map is a bijection. f is termed a *trapdoor* function if the following conditions hold:

1. for every $x \in X$ it is easy (by easy, we mean the number of operations required to evaluate $f(x)$ is small) to determine $f(x)$.
2. for every $f(x) \in Y$ it is difficult to evaluate x.

Trap door Functions

Let $\mathbb{P}$ denote the primes, consider the function

$$f : \mathbb{P} \times \mathbb{P} \to \mathbb{N}, \quad (p_1, p_2) \mapsto_f p_1 p_2; \tag{0.4}$$

in plain terms: we multiply two primes together to form their product. For example if

1. $p_1 = 4575163$ and $p_2 = 4093567$ then $f(p_1, p_2) = 18728736276421$ and (not particularly sophisticated) algorithms can do this multiplication in n^2 steps (n the digit length of p_1 and p_2).
2. the reverse operation: that is, determining p_1 and p_2 from 18728736276421 takes 10^n steps.

so f is quadratic in operation count, but its inverse f^{-1} is exponential in operation count.

Fermat's little theorem

Fermat's little theorem is an interesting result in elementary number theory that is needed in our discussion of the RSA algorithm.

Let p be prime and a any integer then

$$a^p = a \mod p. \tag{0.5}$$

Proof of Fermats Theorem

I would like to present a proof of Fermats theorem, and to do this I need two ideas we have meet before :

1. Equivalence relations.
2. Partitioning.

Equivalence Relation

Fix a set X a relation R is simply a subset of $X \times X$ (the idea really is that simple). An *equivalence relation* is a relation that is

1. reflexive: that is $(x, x) \in R$ for all $x \in X$;
2. symmetric: that is if $(x, y) \in R$ then $(y, x) \in R$;
3. transitive: that is if $(x, y) \in R$ and $(y, z) \in R$ then $(x, z) \in R$;

If that is too abstract, observe that: congruent mod n on the integers $\mathbb{Z}$ is an equivalence relation.

Equivalence Relation Partition Sets

Let R denote an equivalence relation on X and define

$$x^\bullet = \{y \in X \mid (x, y) \in R\} \tag{0.6}$$

then the equivalence relation induces a partition in X. Why? Suppose

$$a \in x^\bullet \cap y^\bullet \tag{0.7}$$

so $(x, a) \in R$ and $(y, a) \in R$.

1. $x^\bullet \subseteq y^\bullet$: pick any $z \in x^\bullet$ then $(z, x) \in R$[symmetric] and as $(x, a) \in R$ and $(a, y) \in R$ [symmetric] then $(x, y) \in R$ [transitive] and $z \in y^\bullet$.
2. $y^\bullet \subseteq x^\bullet$: similar to above

So $x^\bullet = y^\bullet$, a picture would help a lot here.

Let G denote a group and H a subgroup then define $(x, y) \in R$ if and only $xy^{-1} \in H$ this is an equivalence relation. Proof:

1. reflexive: $xx^{-1} = 1 \in H$ [because $1 \in H$]
2. symmetric : if $xy^{-1} \in H$ then $xy^{-1} = h$ and we have $yx^{-1} = h^{-1} \in H$
3. transitive: similar

What is the big deal?

Lagrange's theorem

The size of a group G is denored $|G|$. Recall Lagrange's theorem: if H is a subgroup of a group G then $|H| \mid |G|$; that is the order of any subgroup divides the order of the group. For example if a group has order $12 = 2^2 3$ than any subgroup you find will have order 1, 2, 3, 2^2 or $2^2.3$. This allows us to split a group up via cosets.

Important Result

The previous result says for a group G and a subgroup H then

$$|G| = |H| \times \text{ number of cosets} \quad \text{so} \quad \frac{|G|}{|H|} = \text{ number of cosets.} \tag{0.8}$$

In particular if $|G|$ is a prime we deduce it has no subgroups!

proof of Fermat's little theorem

Proof.

Recall Lagrange's theorem: if H is a subgroup of a group G then $|H| \mid |G|$. The non-zero elements of $\mathbb{F}_p$ are under multiplication $\mod p$ a group, thus the order of any non-zero element divides $p-1$. Pick a $a \in \mathbb{F}_p^*$ then for some $n \in \mathbb{N}$ we have $a^n = 1 \mod p$ with $n \mid p-1$ so $p-1 = mn$

$$a^p = a^{mn+1} = aa^{mn} = a(a^n)^m = a1^m = a \mod p. \tag{0.9}$$

□

Variant

We have

$$a^p = a \mod p \quad \text{and thus} \quad a^{p-1} = 1 \mod p. \tag{0.10}$$

Can we have a go at proving this claim.

Fermat's little theorem

Fermat's little theorem has numerous applications. We mention two:

1. It establishes factorization properties for certain numbers, and some of these results are beyond modern day computing power.
2. It allows a method for constructing the multiplicative inverse in a field.

Fermat's little theorem - 1

Why is Fermat's little theorem so interesting. We look at an example from Hoffstein, consider the prime $p = 15485863$ then Fermat's little theorem (from the 16th century) states

$$2^{15485862} = 1 \quad \text{mod } 15485863 \quad \text{mod } p \qquad (0.11)$$

and thus with no computing we know $2^{15485862} - 1$ is divisible by 15485863; a fact that no computer (in the 21st century) could establish directly. These clever number theory ideas give cryptologists ‘cold sweats’, they live in fear of number theorists!

Inverses using Fermat - 2

Fermat's result

$$a^{p-1} = 1 \mod p. \tag{0.12}$$

implies

$$a^{p-2}a = 1 \mod p, \tag{0.13}$$

and we have a fast way of evaluating the inverse of a, its inverse is a^{p-2} (which we can evaluate quickly using a fast power algorithm).

Euler's formula

We need another technical result. Let p and q be distinct primes and set

$$g = \gcd((p-1),(q-1)) \tag{0.14}$$

then for all a satisfying $\gcd(a, pq) = 1$ we have

$$a^{(p-1)(q-1)/g} = 1 \mod pq \tag{0.15}$$

Proof of Euler

We are told $p \not| \ a$ and $g \mid q - 1$.

$$\begin{aligned} a^{(p-1)(q-1)/g} &= (a^{p-1})^{(q-1)/g} \mod p \\ &= 1^{(q-1)/g} \mod p \qquad (\ a^{p-1} = 1 \mod p) \\ &= 1 \mod p \end{aligned} \tag{0.16}$$

We are told $q \not| \ a$ and $g \mid p - 1$.

$$\begin{aligned} a^{(p-1)(q-1)/g} &= (a^{p-1})^{(q-1)/g} \mod q \\ &= 1^{(q-1)/g} \mod q \qquad (\ a^{p-1} = 1 \mod q) \\ &= 1 \mod q \end{aligned} \tag{0.17}$$

More Euler

We have

$$a^{(p-1)(q-1)/g} = 1 \mod p \quad \text{and} \quad a^{(p-1)(q-1)/q} = 1 \mod q. \tag{0.18}$$

We deduce

$$a^{(p-1)(q-1)/g} - 1 \tag{0.19}$$

is divisible by both p and q thus it is divisible by pq (this is true because p and q are prime)and

$$a^{(p-1)(q-1)/g} - 1 = 0 \mod pq \tag{0.20}$$

and

$$a^{(p-1)(q-1)/g} = 1 \mod pq. \tag{0.21}$$

The RSA algorithm

We have nearly covered all the theory to code the RSA algorithm, it has been very theory heavy so let us look at the actual algorithm and we will return to a few technical details later.

the usual problem

We have the usual problem: Alice and Bob wish to communicate securely across an insecure channel that Eve has access to.

Bob's Public Key

Anybody who wishes to communicate securely with Bob needs his Public Key. Bob picks two primes p and q (p, $q > 2^{1000}$) evaluates $N = pq$ and picks an encryption exponent e, where e satisfies

$$\gcd(e, (p-1)(q-1)) = 1. \tag{0.22}$$

Bob's public key is the tuple (that is, it is a pair of numbers) $K_{B,Pu} = (N, e)$.

What Alice Does - Encryption

Alice has a plaintext message m (m an integer) and evaluates

$$c = m^e \mod N, \tag{0.23}$$

c is the ciphertext sent to Bob.

How Bob Decrypts

Bob solves two equations, first

$$ed = 1 \mod (p-1)(q-1). \tag{0.24}$$

The only term in eqn. 0.24 that Bob does not know is d, so this is simply finding the inverse of $e \mod (p-1)(q-1)$. He then evaluates

$$m' = c^d \mod N \tag{0.25}$$

and we find $m = m'$, and he has determined Alice's message.

ElGamal v. RSA

1. The security of ElGamal is linked to the difficulty in solving
$$a^x = b \mod p, \tag{0.26}$$
a, b and p (p prime) all known, and x is unknown.
2. The security of RSA is linked to the difficulty in solving
$$x^e = c \mod N, \tag{0.27}$$
e, c and N all known, and x is unknown.

Authenticity

Recall the four principles:

1. Confidentiality - The message the recipient gets can be proven not to have been read by anyone else.
2. Integrity - The message the recipient gets can be proven not to have been changed since it was encoded.
3. Authenticity - The message the recipient gets can be proven to have been encoded by a positively-identified sender.
4. Non-repudiation - The sender, given a message received by a recipient, cannot validly deny that the message was sent by him or that it was not the original content sent by him.

Authenticity

I mention (glossing over a few details) that in the real world RSA is not quite done as in this lecture or the lab questions.
The fundamental problem is that everyone has access to $K_{B,Pu}$ (Bob's public key) so when the message arrives from Alice then Bob cannot be sure the message was sent by Alice, it could have been Eve.
The resolution?

Resolution

Alice currently encrypts her plain text message with Bob's public key, what happens in the real world is

1. Alice encrypts her plain text message m with her own private key, denote this message $K_{A,Pr}(m)$
2. Alice then encrypts $K_{A,Pr}(m)$ with Bob's public key to get $K_{B,Pu}(K_{A,Pr}(m))$.
3. Bob can decrypt $K_{B,Pu}(K_{A,Pr}(m))$ to get $K_{A,Pr}(m)$.
4. Bob can use Alice's public key to decrypt $K_{A,Pr}(m)$ to get m.

He is now sure he is talking to Alice because the only person who could have sent the message has access to Alice's private key. This is the 'two way' handshake that allows you and (say) amazon to be sure you are talking to each other

Summary: RSA

1. We have developed most of the theory required to show that the RSA algorithm does encrypt and decrypt correctly.
2. Factorizing $N = pq$ when you N but do not know p or q is a very difficult task, and for that reason RSA is believed to be secure to attack from Eve.