

RSA ENCRYPTION AND DECRYPTION

Section 1. Two Facts from Number Theory

In order to understand RSA encryption we need two ideas from class: the Extended Euclidean Algorithm and the method of successive squaring. We also need two new ideas: Fermat's Little Theorem and the Chinese Remainder Theorem.

Fermat's Little Theorem: If p is prime and a is an integer not divisible by p , then $a^{p-1} \equiv 1 \pmod{p}$.

Example: Let's take $p = 7$ and $a = 3$. Then:

$$3^1 \equiv 3 \pmod{7}$$

$$3^2 \equiv 2 \pmod{7}$$

$$3^3 \equiv 6 \pmod{7}$$

$$3^4 \equiv 4 \pmod{7}$$

$$3^5 \equiv 5 \pmod{7}$$

$$3^6 \equiv 1 \pmod{7}$$

This last line is an example of Fermat's Little Theorem.

Chinese Remainder Theorem Let m_1 and m_2 be two integers with $\gcd(m_1, m_2) = 1$. Let a_1 and a_2 be any integers. Then the system:

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

has exactly one solution $\pmod{m_1 m_2}$.

Example: Solve the system below:

$$x \equiv 4 \pmod{5}$$

$$x \equiv 3 \pmod{11}$$

Solution: List all the integers that are congruent to 3 $\pmod{11}$, up to 5×11 : 3, 14, 25, 36, 47. The only one that is also congruent to 4 $\pmod{5}$ is 14. Since $\gcd(5, 11) = 1$, the Chinese Remainder Theorem guarantees us that $x \equiv 14 \pmod{55}$ is the only solution.

There is a more general version of the Chinese Remainder Theorem, but we don't need it to understand RSA encryption.

Section 2. RSA Encryption

A public encryption key has two parts: n and e . The number n is equal to pq , where p and q are different primes with around 200 digits each. Let ϕ equal $(p-1)(q-1)$. The number e must satisfy $\gcd(e, \phi) = 1$. We translate the message into numbers using A=0, B=1, ..., Z=25. To encrypt each letter M we calculate $M^e \pmod{n}$ using successive squaring. Let's call the encrypted letter C (for ciphertext). We have $C \equiv M^e \pmod{n}$.

Example: Encrypt the message KEYS using the public key $n = 187$ and $e = 7$. Notice that we do not need to know the factorization of n to do this.

Solution: We first translate the numbers into letters: K= 10, E=4, Y= 24, S= 18. We write the message as 010 004 024 018 so that each block has the same length as n . We encrypt each block M using $C \equiv M^7 \pmod{187}$. We can do this part by successive squaring.

$$10^2 \equiv 100 \pmod{187}, 10^4 \equiv 89 \pmod{187} \\ \Rightarrow 10^7 \equiv 89 \cdot 100 \cdot 10 \pmod{187} \equiv 175 \pmod{187}.$$

$$4^2 \equiv 16 \pmod{187}, 4^4 \equiv 69 \pmod{187} \\ \Rightarrow 4^7 \equiv 69 \cdot 16 \cdot 4 \pmod{187} \equiv 115 \pmod{187}.$$

$$24^2 \equiv 15 \pmod{187}, 24^4 \equiv 38 \pmod{187} \\ \Rightarrow 24^7 \equiv 38 \cdot 15 \cdot 24 \pmod{187} \equiv 29 \pmod{187}.$$

$$18^2 \equiv 137 \pmod{187}, 18^4 \equiv 69 \pmod{187} \\ \Rightarrow 18^7 \equiv 69 \cdot 137 \cdot 18 \pmod{187} \equiv 171 \pmod{187}.$$

The encrypted ciphertext is 175 115 029 171.

Section 3. RSA Decryption

Recall that $\phi = (p-1)(q-1)$. Because $\gcd(e, \phi) = 1$, there exist integers d and k so that $de - k\phi = 1$. The number d is the private decryption key. To decrypt a message we calculate $C^d \pmod{n}$.

Example: Decrypt the ciphertext 175 115 029 171 using $n = 187$ and $e = 7$ to confirm that the original message is found.

Solution: We first need to factor n . We run through the list of primes: 2, 3, 5, 7, 11, 13, ... until we find a divisor of n . We find that $n = 11 \cdot 17$. This means that $\phi = 10 \cdot 16 = 160$. Since $\gcd(7, 160) = 1$ we can use the Extended Euclidean Algorithm to find integers d and k so that $7d - 160k = 1$.

$$\begin{aligned} 160 &= 22(7) + 6 \\ 7 &= 1(6) + 1 \end{aligned}$$

Now working backwards:

$$\begin{aligned} 1 &= 7 - 1(6) \\ &= 7 - 1(160 - 22(7)) \\ &= 23(7) - 1(160) \end{aligned}$$

This tells us that the private decryption key is $d = 23$.

We decrypt using $M \equiv C^{23} \pmod{187}$.

$$175^2 \equiv 144 \pmod{187}, 175^4 \equiv 166 \pmod{187}$$

$$175^8 \equiv 67 \pmod{187}, 175^{16} \equiv 1 \pmod{187}$$

$$\Rightarrow 175^{23} \equiv 1 \cdot 166 \cdot 144 \cdot 175 \pmod{187} \equiv 10 \pmod{187}.$$

$$115^2 \equiv 135 \pmod{187}, 115^4 \equiv 86 \pmod{187}$$

$$115^8 \equiv 103 \pmod{187}, 115^{16} \equiv 137 \pmod{187}$$

$$\Rightarrow 115^{23} \equiv 137 \cdot 86 \cdot 135 \cdot 115 \pmod{187} \equiv 4 \pmod{187}.$$

$$29^2 \equiv 93 \pmod{187}, 29^4 \equiv 47 \pmod{187}$$

$$29^8 \equiv 152 \pmod{187}, 29^{16} \equiv 103 \pmod{187}$$

$$\Rightarrow 29^{23} \equiv 103 \cdot 47 \cdot 93 \cdot 29 \pmod{187} \equiv 24 \pmod{187}.$$

$$171^2 \equiv 69 \pmod{187}, 171^4 \equiv 86 \pmod{187}$$

$$171^8 \equiv 103 \pmod{187}, 171^{16} \equiv 137 \pmod{187}$$

$$\Rightarrow 171^{23} \equiv 137 \cdot 86 \cdot 69 \cdot 171 \pmod{187} \equiv 18 \pmod{187}.$$

We retrieve the original message: 010 004 024 018, which in letters is KEYS.

This confirms that the encryption/decryption algorithm works in this case.

Section 4. Why The Decryption Algorithm Works

Recall that in the decryption algorithm we find d by solving

$de - k(p-1)(q-1) = 1$. When we decrypt, we calculate

$$C^d \equiv (M^e)^d \equiv M^{1+k(p-1)(q-1)} \pmod{n}.$$

By Fermat's Little Theorem, $M^{(p-1)} \equiv 1 \pmod{p}$ so

$$M^{1+k(p-1)(q-1)} \equiv M \cdot (M^{(p-1)})^{k(q-1)} \equiv M \cdot 1 \equiv M \pmod{p}. \quad (*)$$

Similarly, $M^{1+k(p-1)(q-1)} \equiv M \pmod{q}. \quad (**)$

Now by the Chinese Remainder Theorem, since $\gcd(p, q) = 1$ (p and q are different primes), there is exactly one number \pmod{pq} that has properties $(*)$ and $(**)$ —it is $M \pmod{pq}$. So $C^d \equiv M \pmod{pq}$, or in other words $C^d \equiv M \pmod{n}$. The message has been decrypted.

The one extra requirement for the decryption algorithm to work is that $\gcd(M, p)$ and $\gcd(M, q)$ must equal 1. One way to guarantee this is to ensure that the blocks of the message have fewer digits than p or q .

The security of the RSA algorithm rests on the fact that $n = pq$ is extremely difficult to factor. Without factoring n , there is no (known) way to find the private decryption key d .

Section 5. Exercise

A message is encrypted with RSA using $n = 247$ and $e = 31$. The encrypted message reads 045 199 106 219. What is the original message?

Let's find the answer step by step.

- a) Factor $n = 247$ as the product of two primes.
- b) Compute $\phi = (p - 1)(q - 1)$.
- c) Find d so that $ed - k\phi = 1$. To do this we perform the Euclidean algorithm on ϕ and $e = 31$. Then we work backwards. The k is irrelevant, but the d is the private decryption key.
- d) Now that d is known, we can decrypt each block C in the ciphertext by computing $C^d \pmod{247}$. The fastest way to do this is by successive squaring: Compute C^2, C^4, \dots by successively squaring the previous number and reducing mod 247.
- e) The final step is to convert each decrypted number to a letter. We reduce mod 26 to find the letter. A table is provided below for your convenience:

00	01	02	03	04	05	06	07	08	09	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M
13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z