RSA Cryptosystems

Encryption is the process of encoding information. This process converts the original representation of the information, known as **plaintext**, into an alternative form known as **ciphertext**. Ideally, only authorized parties can decipher a ciphertext back to plaintext and access the original information.

Example 1. Simple **substitution ciphers** work by replacing each plaintext character by another one character. To decode ciphertext letters, one should use a reverse substitution and change the letters back.

Before messages can be send, one needs to agree how the letters are shuffled. This is a bijection on the set of letters:

```
ABCDE FGHIJ KLMNO PQRST UVWXYZ
KXONZ IHCRE TUAMD SVJFG PBLWQY
```

Because there are 26 letters in English alphabet, there a 26! different ways to order the letters. In addition 26! is quite big number: 403291461126605635584000000, consisting of 27 digits. So, checking all possible combinations would take some time. However, checking all the combinations is not possible.

This kind of substitution method suffers from the fact that the same letter is always encrypted the same way. This means that `E` is always encrypted as `Z`, `A` is encrypted as `K`, and so on. In Figure 1, the frequencies of letters in English letters are presented. This means, for instance, that the most frequent letter in the cipher text correspond `E`, and so. If one tries combinations of the most frequent letters, some meaningful words start to appear.

In **symmetric key cryptography**, both parties must possess a secret key which they must **exchange** prior to using any encryption. Distribution of secret keys has been problematic until recently, because it involved face-to-face meeting, use of a trusted courier, or sending the key through an existing encryption channel. The first two are often impractical and always unsafe, while the third depends on the security of a previous key exchange.

In **public key cryptography**, the key distribution of public keys is done through public key servers. When a person creates a key-pair, they keep the *private key* and the other, known as the *public-key*, is uploaded to a server where it can be accessed by anyone to send the user an encrypted message.

The RSA algorithm is an asymmetric cryptography algorithm; this means that it uses a public key and a private key (i.e two different, mathematically linked keys). As their names suggest, a public key is shared publicly, while a private key is secret and must not be shared with anyone.

The RSA algorithm is named after those who invented it in 1978: Ron Rivest, Adi Shamir, and Leonard Adleman. We first describe RSA algorithm and then present the mathematical statement to validate.

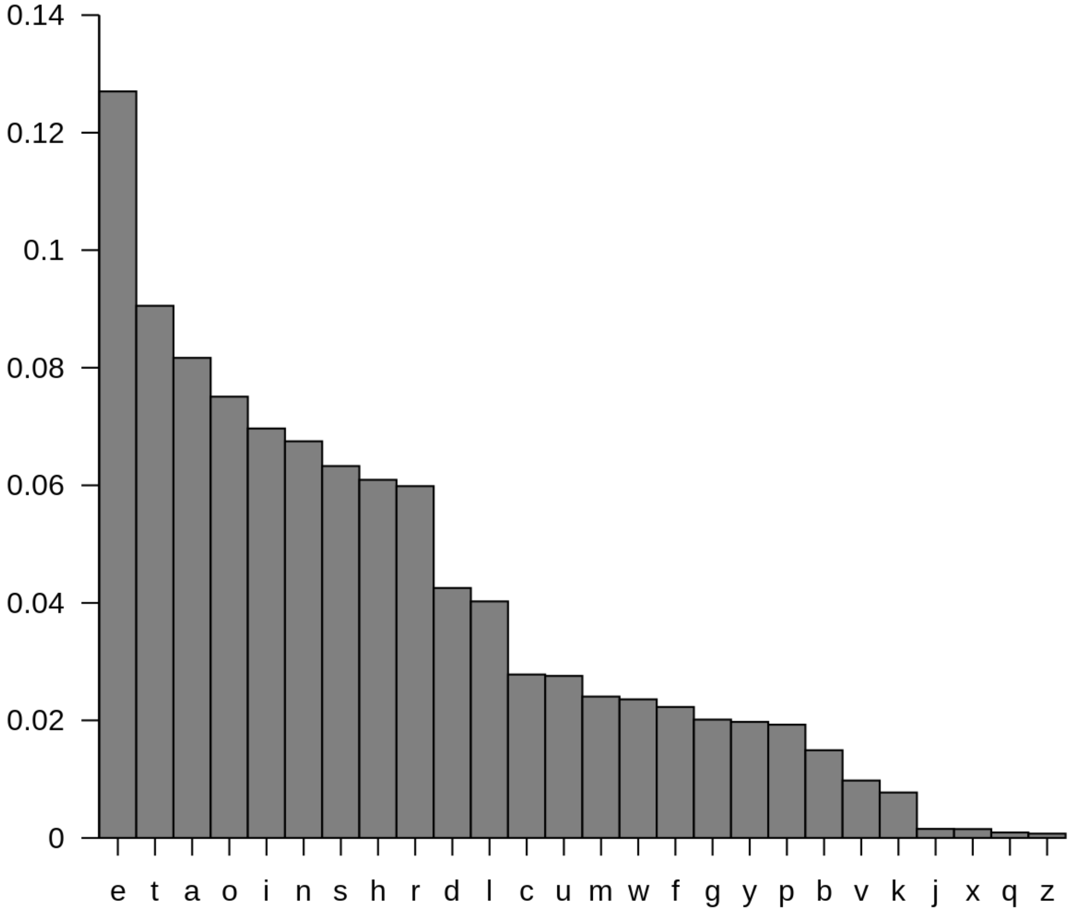
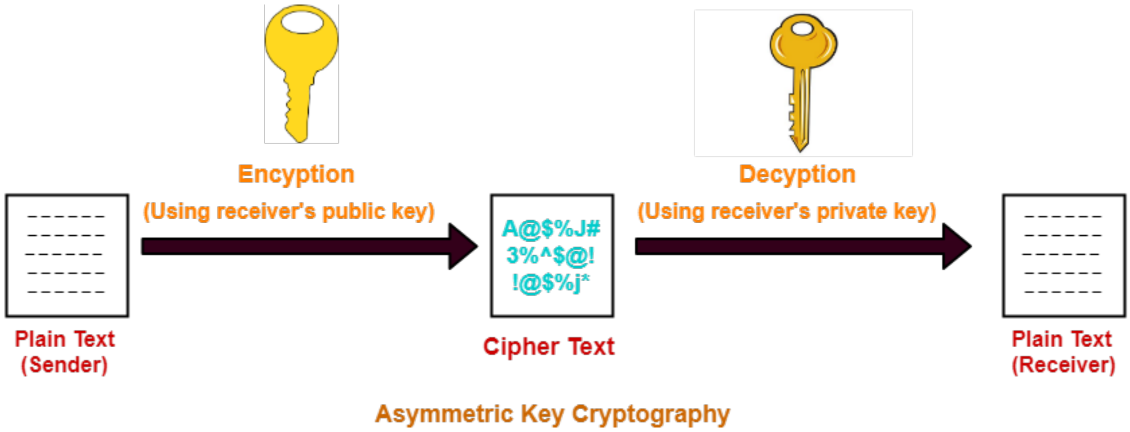


Figure 1: English letter frequency



Step 1 (at sender side):

- Sender encrypts the message using receiver's public key.
- The public key of receiver is publicly available and known to everyone.
- Encryption converts the message into a cipher text.
- This cipher text can be decrypted only using the receiver's private key.

Step 2:

- The cipher text is sent to the receiver over the communication channel.

Step 3 (at receiver side):

- Receiver decrypts the cipher text using his private key.
- The private key of the receiver is known only to the receiver.
- Using the public key, it is not possible for anyone to determine the receiver's private key.
- After decryption, cipher text converts back into a readable format.

Mathematically, the process is the following:

1. Let $n = p \cdot q$, where p and q are two prime numbers. These numbers must be kept secret. We set
$$\phi = (p-1) \cdot (q-1).$$
2. Choose an integer e with $1 < e < n$ such that e and ϕ are *relatively prime*, that is, $\gcd(\phi, e) = 1$.

3. The public key consists of n and e where e is the encryption key.

   Once it is published, anyone can use it to encrypt messages. The encrypted message C is computed as
   $$C = \text{rem}(M^e, n),$$
   where M is the original message as an integer $0 < M < n$. Note that C is now an integer $0 < C < n$ such that $C \equiv M^e \bmod n$.

4. The private key is a positive integer d that satisfies:
   $$d \cdot e \equiv 1 \bmod \phi$$

5. Once the creator of the public key receives an encrypted message C, he or she uses the following decryption function to obtain the original message M by computing:
   $$M = \text{rem}(C^d, n)$$

The *multiplicative inverse* of $x \in \mathbb{R}$ is a number y such that:
$$x \cdot y = 1.$$
Multiplicative inverses exist over the real numbers. For example, the multiplicative inverse of 3 is 1/3 since:
$$3 \cdot \frac{1}{3} = 1.$$
The only exception is that 0 does not have an inverse.

Multiplicative inverses generally *do not exist over the integers.* For example, 7 can not be multiplied by another integer to give 1.

But multiplicative inverses do exist when we are working modulo a *prime number.* For example, if we are working modulo 5, then 3 is a multiplicative inverse of 7, since:
$$7 \cdot 3 = 21 \equiv 1 \bmod 5$$

Lemma 2. *If ϕ and e are relatively prime, then e has a multiplicative inverse modulo ϕ.*

Proof. Because ϕ and e are relatively prime, $\gcd(\phi, e) = 1$. Therefore, there is a linear combination of ϕ and e equal to 1, that is,
$$k_1\phi + k_2 e = 1.$$
Rearranging terms gives:
$$k_1\phi = 1 - k_2 e.$$
This implies that $\phi | (1 - k_2 e)$ by the definition of divisibility, and therefore $k_1 e \equiv 1 \bmod \phi$ by the definition of congruence. This means that k_1 is a multiplicative inverse of e. □

Example 3. Let two primes be $p = 61$ and $q = 53$. Compute $n = pq = 61 \times 53 = 3233$. We have that $\phi = 60 \times 52 = 3120$.

Let $e = 173$. We compute $\gcd(3120, 173)$:

$$\begin{array}{lll} 3120 & = 18 \times 173 + 6 & \gcd(3120, 173) = \gcd(173, 6) \\ 173 & = 28 \times 6 + 5 & \gcd(173, 6) = \gcd(6, 5) \\ 6 & = 1 \times 5 + 1 & \gcd(6, 5) = \gcd(5, 1) \\ 5 & = 5 \times 1 + 0 & \gcd(1, 0) = 1 \end{array}$$

So, $\gcd(3120, 173) = 1$ and ϕ and e are relatively prime, as required.

Suppose that $M = 65$. The encrypted message is

$$\mathrm{rem}(65^{173}, 3233).$$

Now 65^{173} is

```
4305372170116571994639391671528436440316518639633542874382267053149178
5076800568702732560848392332220242462767546746974644093887541996522536
1571342564165056796187106079728279967290726334736935613377682277806215
6982693310399597324610217758955503934475677935786812739752586840641379
5952403233968652784824371337890625
```

Its remainder is 405 when divided by 3233.

Because we are using modulo arithmetics, the computation of remainders is actually easier at is first seems.

Lemma 4. *Let a, b and $n > 1$ be integers.*

$$\mathrm{rem}(ab, n) = \mathrm{rem}(\mathrm{rem}(a, n) \cdot \mathrm{rem}(b, n), n)$$

Proof. Let us write $r_1 = \mathrm{rem}(a, n)$ and $r_2 = \mathrm{rem}(b, n)$. Then

$$a = k_1 \cdot n + r_1 \quad \text{and} \quad b = k_2 \cdot n + r_2$$

for some integers k_1 and k_2. We have

$$\begin{aligned} a \cdot b &= (k_1 \cdot n + r_1)(k_2 \cdot n + r_2) \\ &= (k_1 k_2 n^2 + k_1 n r_2 + k_2 n r_1 + r_1 r_2) \\ &= n(k_1 k_2 n + k_1 r_2 + k_2 r_1) + r_1 r_2 \end{aligned}$$

This gives that $\mathrm{rem}(ab, n) = \mathrm{rem}(r_1 r_2, n)$, which completes the proof. □

Corollary 5. *Let M, $e > 0$, and $n > 0$ be integers. Then,*

$$\operatorname{rem}(M^e, n) = \operatorname{rem}(\operatorname{rem}(m, n)^e, n).$$

Proof. We can use Lemma 4 repeatedly. This means that

$$\begin{aligned}
\operatorname{rem}(M^e, n) &= \operatorname{rem}(\underbrace{M \cdot M \cdots M}_{e \text{ times}}, n) \\
&= \operatorname{rem}\big(\underbrace{\operatorname{rem}(M, n) \cdot \operatorname{rem}(M, n) \cdots \operatorname{rem}(M, n)}_{e \text{ times}}, n\big) \\
&= \operatorname{rem}(\operatorname{rem}(M, n)^e, n)
\end{aligned}$$

□

Example 6. Let us compute some remainders of powers.

(a) $\operatorname{rem}(10^{100}, 3) = \operatorname{rem}(\operatorname{rem}(10, 3)^{100}, 3) = \operatorname{rem}(1^{100}, 3) = \operatorname{rem}(1, 3) = 1$.

(b) This is more complicated:

$$\operatorname{rem}(5^{32}, 7) = \operatorname{rem}((5^2)^{16}, 7) = \operatorname{rem}(\operatorname{rem}(25, 7)^{16}, 7) = \operatorname{rem}(4^{16}, 7) = \operatorname{rem}(\operatorname{rem}(4^2, 7)^8, 7)$$
$$= \operatorname{rem}(16, 7)^8, 7) = \operatorname{rem}(2^8, 7) = \operatorname{rem}(\operatorname{rem}(2^4, 7)^2, 7) = \operatorname{rem}(\operatorname{rem}(16, 7)^2, 7) =$$
$$\operatorname{rem}(2^2, 7) = 4.$$

(c) In Python, there is command

```
pow(x,e,m)
```

to compute $\operatorname{rem}(x^e, m)$ efficiently. Now,

```
>>> pow(5,32,7)
4
```

For decoding, we need to know the multiplicative inverse of e. In the above, we used Eucleidean algorithm to show that $\gcd(3120, 173) = 1$.

We can now write the remainders in terms or 3120 and 173:

$$6 = 3120 - 18 \times 173$$

$$\begin{aligned}
5 &= 173 - 28 \times 6 \\
&= 173 - 28(3120 - 18 \times 173) \\
&= 173 - 28 \times 3120 - 28 \times 18 \times 173 \\
&= 173 - 28 \times 3120 - 504 \times 173 \\
&= -28 \times 3120 + 505 \times 173
\end{aligned}$$

$$\begin{aligned}
1 &= 6 - 5 \\
&= 3120 - 18 \times 173 + 28 \times 3120 - 505 \times 173 \\
&= \boxed{29 \times 3120 - 523 \times 173}
\end{aligned}$$

From the ASCII table...

Symbol	Decimal	Binary
A	65	01000001
B	66	01000010
C	67	01000011
D	68	01000100
E	69	01000101
F	70	01000110
G	71	01000111
H	72	01001000
I	73	01001001
J	74	01001010
K	75	01001011
L	76	01001100
M	77	01001101
N	78	01001110
O	79	01001111
P	80	01010000
Q	81	01010001
R	82	01010010
S	83	01010011
T	84	01010100
U	85	01010101
V	86	01010110
W	87	01010111
X	88	01011000
Y	89	01011001
Z	90	01011010

Symbol	Decimal	Binary
a	97	01100001
b	98	01100010
c	99	01100011
d	100	01100100
e	101	01100101
f	102	01100110
g	103	01100111
h	104	01101000
i	105	01101001
j	106	01101010
k	107	01101011
l	108	01101100
m	109	01101101
n	110	01101110
o	111	01101111
p	112	01110000
q	113	01110001
r	114	01110010
s	115	01110011
t	116	01110100
u	117	01110101
v	118	01110110
w	119	01110111
x	120	01111000
y	121	01111001
z	122	01111010

Table 1: Part of ASCII coding

Now -523 is the multiplicative inverse of $e = 173$. Because each element congruent to -523 modulo $\phi = 3120$ is also a multiplicative inverse, we may select d as the smallest positive such element. Now $d = -523 + 3120 = 2597$. This d is our secret *decryption key*. The original message can now be decrypted as

$$M = \mathrm{rem}(C^d, n) = \mathrm{rem}(405^{2597}, 3233) = 65.$$

Note that every positive integer congruent to 2597 modulo ϕ works, for instance

$$\mathrm{rem}(405^{5717}, 3233) = 65.$$

How to encode text to numbers? For instance, a part of ASCII coding is given in the Table 1. See also, for instance, `https://onlineasciitools.com/convert-ascii-to-decimal`

For instance, the word "Math" corresponds to decimal numbers 77,97,116,104. The simplest way is just do consider it as a number

$$7797116104.$$

Note that since $M < n$, the text needs to be divided into blocks of suitable size.

Before proving the correctness of RSA algorithm, we need some additional facts.

Lemma 7. *Let M be an integer. If $p \neq q$ are primes such that*

$$a \equiv M \bmod p \qquad \textit{and} \qquad a \equiv M \bmod q,$$

then

$$a \equiv M \bmod pq.$$

Proof. Now

$$a = M + pk_1 = M + qk_2$$

for some k_1 and k_2. Therefore,

$$pk_1 = qk_2$$

This means that $p|qk_2$. By Euclid's Lemma (Lemma 10 of 'Number Theory'), this means that $p|q$ or $p|k_2$. Because p and q are primes, we must have $p|k_2$, and so $k_2 = pk_3$ for some integer k_3. Now

$$a = M + qk_2 = M + qpk_3$$

This means that $a - M = k_3pq$ and

$$a \equiv M \bmod pq.$$

□

Theorem 8 (Fermat's Little Theorem). *If a is an integer and p is a prime number, then*

$$a^p \equiv a \bmod p.$$

Proof. We prove this theorem is by induction with respect to a. Let p as a prime number. The base case when $a = 1$ is obviously true, because $1^p = 1 \equiv 1 \bmod p$,

Suppose the statement $a^p \equiv a \bmod p$ is true. We show that the statement folds for $a + 1$. By the binomial theorem,

$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \cdots + \binom{p}{p-1} a + 1. \qquad (**)$$

Note that for $1 \leq k \leq p - 1$,

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{(k+1)(k+2)\cdots(p-1)p}{1 \cdot 2 \cdots (k-1)k}.$$

This means that p divides the numerator, but not the denominator. Therefore,

$$\binom{p}{k} \equiv 0$$

for all $1 \leq k \leq p-1$. We get from (**) that

$$(a+1)^p \equiv a^p + 1 \bmod p.$$

Since by the induction hypothesis $a^p \equiv a \bmod p$, we have

$$(a+1)^p \equiv a + 1 \bmod p,$$

as desired. $\square$

The following gives an equivalent formulation of Fermat's Little Theorem if $p \nmid a$.

Lemma 9. *Let a be an integer and p a prime such that $p \nmid a$.*

$$a^{p-1} \equiv 1 \bmod p \iff a^p = a \bmod p.$$

Proof. ($\Rightarrow$) If $p|(a^{p-1}-1)$, then clearly $p|a \cdot (a^{p-1}-1) = a^p - a$.
($\Leftarrow$) Suppose $p|a^p - a = a(a^{p-1}-1)$. This implies that $p|a$ or $p|(a^{p-1}-1)$. But by assumption, $p|a$ is not possible. So, $p|(a^{p-1}-1)$. $\square$

We can now prove the following proposition stating that the message can be read correctly after encryption and decryption.

Proposition 10.

$$(M^e)^d \equiv M \bmod n.$$

Proof. Let us first note that e and d are multiplicative inverses modulo ϕ, that is, $ed \equiv 1 \bmod \phi$. Therefore, there is an integer k such that $ed = (p-1)(q-1)k + 1$ and $ed - 1 = (p-1)(q-1)k$. Moreover, this means that

$$ed - 1 = (p-1)h = (q-1)l$$

for some nonnegative integers h and l.

We show that

$$(M^e)^d \equiv M \bmod p \qquad \text{and} \qquad (M^e)^d \equiv M \bmod q$$

This then proves by Lemma 7 that

$$(M^e)^d \equiv M \bmod n,$$

recall that $n = pq$. Note also that based on exponentiation rules, $(M^e)^d = M^{ed}$.

We consider two cases (i) $M \equiv 0 \bmod p$ and $M \not\equiv 0 \bmod p$.

(i) Let $M \equiv 0 \bmod p$. Then $M = pk$ for some integer k. Thus,

$$M^{ed} = (pk)^{ed} = p \cdot p^{ed-1} k^{ed}.$$

This means that M and M^{ed} are both multiples of p and $(M^e)^d \equiv M \bmod p$.

(ii) Let $M \not\equiv 0 \bmod p$. This means that M is not divisible by p. Then, $M^{p-1} \equiv 1 \bmod p$ by Lemma 9. We have

$$M^{ed} = M^{ed-1}M = M^{h(p-1)}M = (M^{p-1})^h M.$$

Now

$$\mathrm{rem}\left((M^{p-1})^h, p\right) = \mathrm{rem}\left(\mathrm{rem}(M^{p-1}, p)^h, p\right) = \mathrm{rem}(1^h, p) = \mathrm{rem}(1, p) = 1.$$

This implies that

$$\mathrm{rem}((M^{p-1})^h M, p) = M.$$

This means that $(M^e)^d \equiv M \bmod p$.

By replacing every instance of "p" by "q", we can show that $(M^e)^d \equiv M \bmod q$. As we already noted, these two equations imply that

$$(M^e)^d \equiv M \bmod n. \qquad \square$$

Remember that we first encrypted the message by

$$C = \mathrm{rem}(M^e, p).$$

Then, the message is decrypted by

$$D = \mathrm{rem}(C^d, p).$$

We have that

$$\begin{aligned} D &= \mathrm{rem}(C^d, p) \\ &= \mathrm{rem}(\mathrm{rem}(M^e, p)^d, p) \\ &= \mathrm{rem}((M^e)^d, p) \end{aligned}$$

This means that $D \equiv M \bmod p$. Because $0 < M < n$ and $0 < D < n$, we have $D = M$, meaning that the text is decrypted correctly.