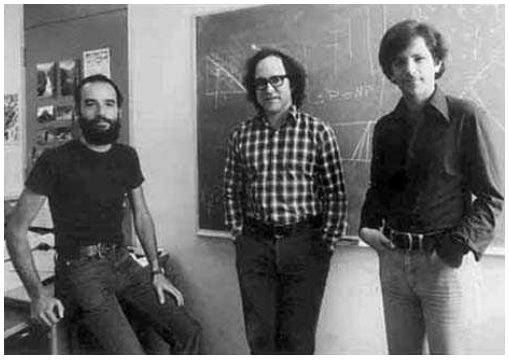
1. 什么是 RSA

根据密钥的使用方法，可将密码分为对称密码和公钥密码。

对称密码：加密和解密使用同一种密钥，发送方（加密）和接收方（解密方）都知道密码。

公钥密码：加密和解密使用不同的密钥，发送方（加密）和接收方（解密方）所用密码不同，接收方掌握的私钥密码不必让发送方知道。



Rivest、Shamir 和 Adleman

RSA 算法是现今使用最广泛的公钥密码算法，也是号称地球上最安全的加密算法。1977 年，由 Rivest、Shamir 和 Adleman 提出。

2. RSA 加密

$$密文 = 明文^{E} \bmod N$$

密文是明文的 E 次方除以 N 的余数。E、N是 RSA 加密的密钥，称为**公钥**。公钥是对外公开的。

$$公钥 = (E, N)$$

E 是加密（Encryption）的首字母。

3. RSA 解密

$$明文 = 密文^{D} \bmod N$$

密文的 D 次方除以 N 的余数就是解密后的明文；D 和 N 的组合就是私钥（用来解密）

$$私钥 = (D, N)$$

此处 D 是解密（Decryption）的首字母。

(E, D, N)要精心选择，才能实现加密和解密。

4. 生成密钥对(E, D, N)

密钥对是怎样生成的？步骤如下：

1、求N	2、求中间数L	3、求E	4、求D

4.1 求N

准备两个质数 p, q。这两数不能太小，否则会容易破解，令

$$N = p \times q$$

4.2 求中间过程数L

L 是 $p-1$ 和 $q-1$ 的最小公倍数，即

$$L = \mathrm{lcm}(p-1, q-1)$$

4.3 求E

E 必须满足两个条件：	$\mathbf{1} < E < L$ $\mathbf{gcd}(E, L) = \mathbf{1}$

其中，$\gcd(X, Y)$为 X 和 Y 的最大公约数；由此生成公钥(E, N)。第二个条件表明，E 和 L 互质。

4.4 求D

D 也必须满足两个条件：	$\mathbf{1} < D < L$ $\boldsymbol{E \times D \bmod L = 1}$

由此生成私钥(D, N)。

5 实例

我们使用较小的数字来模拟。

5.1 求 N

准备一对质数， p = 5 ；q = 11；N = p * q = 55

5.2 求 L

L = lcm（p - 1， q - 1）= lcm(4，10） = 20

5.3 求 E

E 必须满足 2 个条件：1 < E < L ，gcd（E，L）=1，即

1 < E < 20，gcd（E，20） = 1

可取 E = 3

公钥 = (E，N） = （3，55）

5.4 求 D

D 也必须满足 2 个条件：1 < D < L，E * D mod L = 1，即

1 < D < 20，3 * D mod 20 = 1

显然当 D = 7 时满足上述两个条件，所以

私钥 =（D，N）=（7，55）

5.5 加密与解密

明文应小于 N，设 明文 = 12

则 密文 = 明文 $^{E} mod\ N = 12^{3} mod\ 55 = 23$

5.6 解密

明文 = 密文 $^{D} mod\ N = 23^{7} mod\ 55 = 12$

解密后的明文为 12，和原来的明文一致！