# Shor’s Algorithm

## 第2讲： RSA加密机制

# 1. 了解RSA的算法规则

本源量子

本源量子

# RSA算法

## 生成密钥：

1. 生成两个大质数$p$和$q$ 。
2. 计算$n = p \times q$，以及$\varphi = (p-1) \times (q-1)$
3. 选择一个随机数$1 < e < \varphi$ ，形如： $gcd(e, \varphi) = 1$
4. 计算唯一的整数$1 < d < \varphi$ , 形如： $e \times d = 1\ (mod\ \varphi)$
5. $(d, n)$是私钥。
6. $(e, n)$是公钥。

## 加密

1. 讯息$m$用区间$[0, n-1]$的整数来表示。
2. 通过加密得到数据$c$，然后发送$c$

$$\mathrm{c} = m^{\mathrm{e}} \bmod n$$

## 解密

1. 解密钥：

$$\mathrm{m} = c^{d}\ mod\ n$$

本源量子

# 基础知识 | gcd原理

$$\gcd\left(N_1, N_2\right)$$

(Greatest common divisor)

求$N_1, N_2$的最大公因数算法。

$gcd\left(N_1, N_2\right) = 1$，则称$N_1, N_2$互质。

**例：** 求$\gcd(12, 24)$？

- 数字24可以表示为几组不同正整数的乘积

$$24 = 1 \times 24 = 2 \times 12 = 3 \times 8 = 4 \times 6$$

故24的正因数为:**1，2，3，4，6，8，12，24**

- 数字12可以表示为几组不同正整数的乘积

$$12 = 1 \times 12 = 2 \times 6 = 3 \times 4$$

故12的正因素为**1，2，3，4，6，12**

- 两组数中，共同的元素，就是它们的公因数:

**1，2，3，4，6，12**

- 其中的最大数12即为12和24的最大公因数.

记为：$\gcd(12, 24) = 12$

本源量子

# 基础知识 | mod运算

## $\boldsymbol{mod}$（a, $\boldsymbol{b}$）

### 求模运算符

例如$a$ mod $b = c$，表明$a$除以$b$余数为$c$

mod **12**

1 **mod** 12 = 1

4 **mod** 12 = 4

20 **mod** 12 = 8

25 **mod** 12 = 1

### 模运算满足：

$$ab\ mod\ N = [(a\ mod\ N) \times (b\ mod\ N)]\ mod\ N$$

$$5^3\ mod\ 11$$

$$= 5^2 \times 5 \bmod 11$$

$$= 25 \times 5\ mod\ 11$$

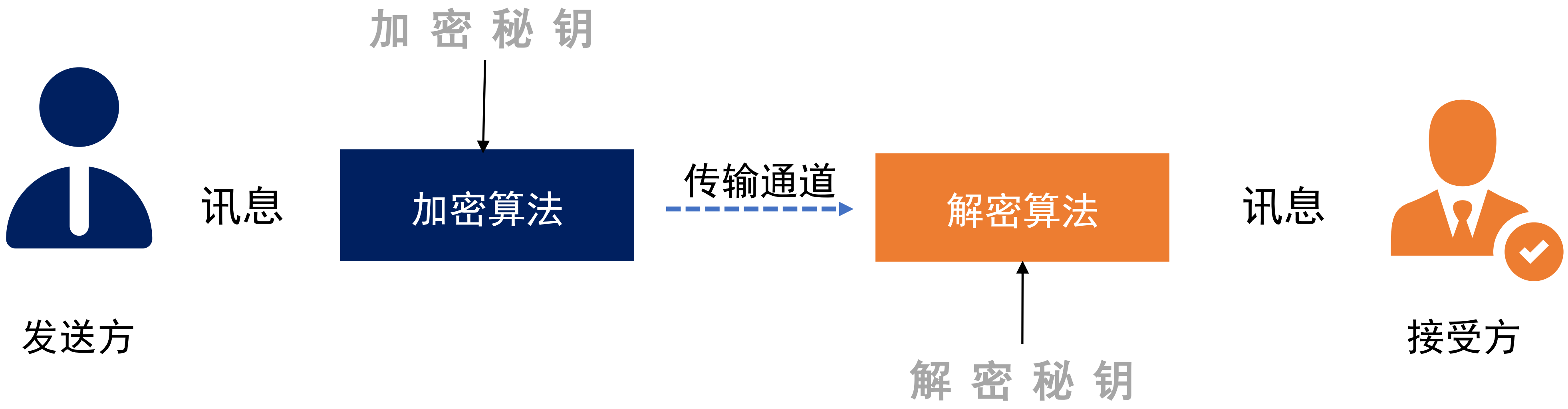
$$= 3 \times 5 \bmod 11$$

$$= 15\ mod\ 11 = 4$$

**问题转化为：** $f(r) = a^r \bmod \mathrm{N}$

本 源
量 子

# RSA加密简单原理



本源量子

# RSA加密演示

| A | B | … | Z | … |
| --- | --- | --- | --- | --- |
| 65 | 66 | … | 90 | 91… |

比如：我要把**BY**字母从上海发回合肥！

本源量子

# RSA加密演示

明　　文：　B　　　　Y

字符串T：　66　　　　89

构造公钥和私钥：取 $p=103$ , $q = 97$，

于是构建公钥为 $(e,n) = (1213,\ 9991)$，私钥为 $(d,n) = (4117,9991)$

加密信息

$C_1 = 66^{1213} \bmod 9991 = 8151$

$C_2 = 89^{1213}\ mod\ 9991$ =176

$$c = m^{e} \bmod n$$

本 源
量 子

# RSA加密演示

发回总部的数字： 8151 176

总部操作

解密私钥

私钥为 $(d, n) = (4117, 9991)$

$$\mathrm{m} = c^{d}\ mod\ n$$

$$\mathrm{m}_1 = 8151^{4117}\ mod\ 9991 = 66$$

$$\mathrm{m}_2 = 176^{4117}\ \mathrm{mod}\ 9991 = 89$$

恢 复 明 文: B Y

# 2. 用Shor算法破解RSA

本 源 量 子

本源
量子

# Shor算法破解RSA加密

1994年

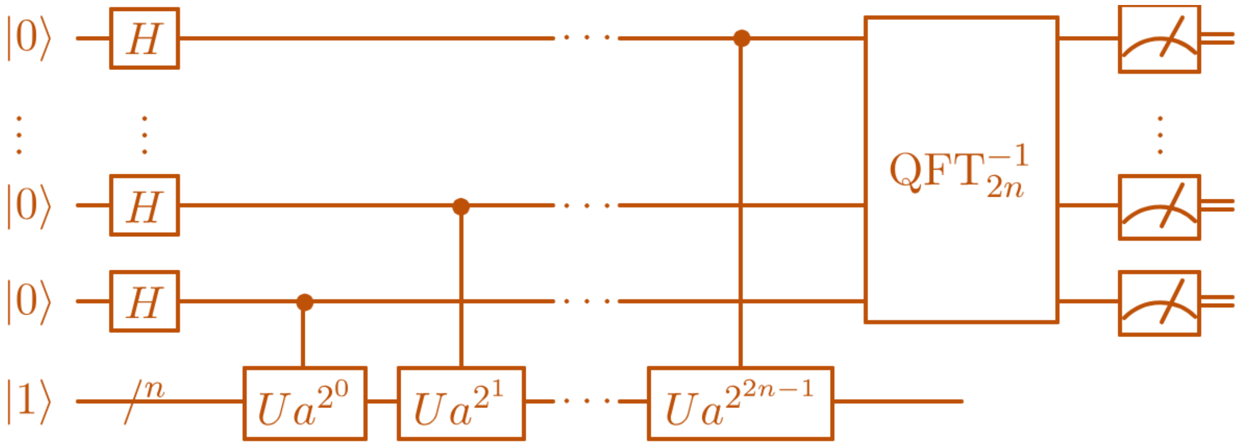
# 量子算法| 整数分解算法（Shor Algorithm）

**需求描述：** 给定一个整数$N$，找出它的质因数。

**算法分析：** 没有已知传统的算法可以在多项式时间内解决这个问题，Shor算法展示了因数分解这个问题可以在在量子计算机上很有效率的分解。

**应用场景：**

- 打破RSA公开密钥体系




参考线路图，量子部分，主要帮助我们寻找到周期

# Shor算法

该算法主要是为了解决**大数的质因数分解问题**！

## 经典部分

## 量子部分

1. 随机选择任意数字$1 < a < N$
2. 计算$\gcd(a, N)$。使用经典算法完成。
3. 如果$\gcd(a, N) \neq 1$，则返回到第1步.
4. 当$\gcd(a, N) = 1$时，构造函数$f(x) = a^x \ mod\ N$。寻找最小周期$r$,使得$f(x + r) = f(x)$.（**量子计算部分**）
5. 如果得到找到的r是奇数，回到第1步。
6. 如果$a^{\frac{r}{2}} = -1 \ (mod\ N)$, 同样回到第1步，从新开始选择$a$.
7. 如果$a^{\frac{r}{2}} \neq -1 \ (mod\ N)$, 则$\gcd(a^{\frac{r}{2}} \pm 1, N)$即为所求。分解完成。

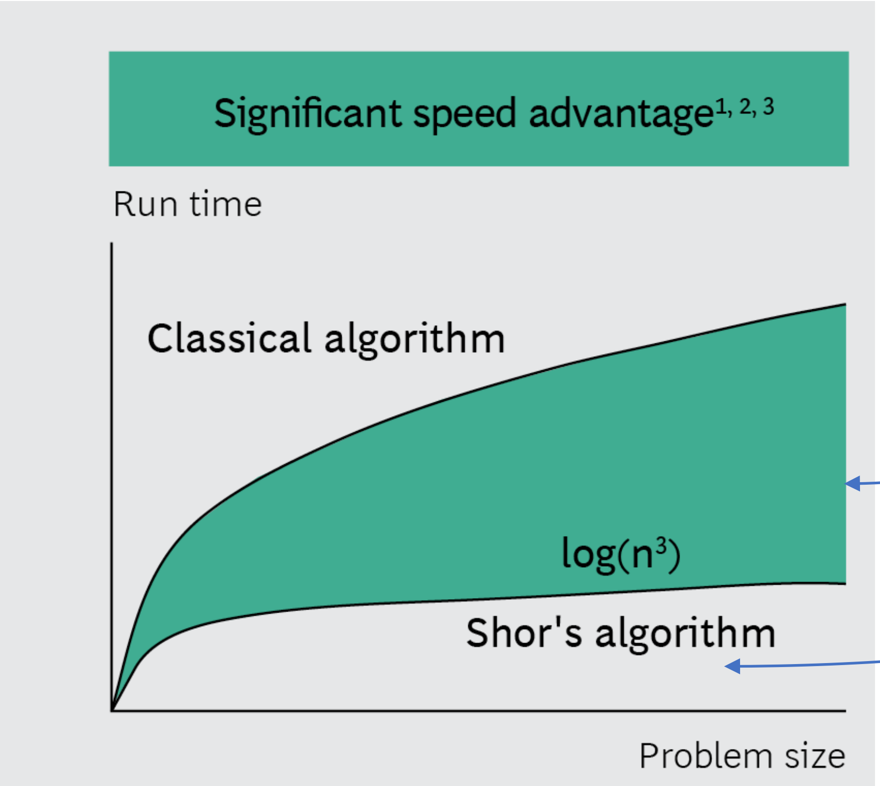
$$N = p \cdot q$$

$$p = \gcd(a^{\frac{r}{2}} + 1, N)$$

$$q = \gcd(a^{\frac{r}{2}} - 1, N)$$

# 量子算法效能比较






经典算法

量子算法

本源
量子

追本溯源 高掌远跖

https://www.originqc.com.cn