海贼宝藏
专注IT教育在线学习平台

金融系统中的 RSA 算法

胡船长
初航我带你，远航靠自己

RSA 算法简史

大约用时：（10 mins）

下一部分：对称加密与非对称加密

Clifford Cocks

1973年英国政府通讯总部工作的Clifford Cocks发明了一种非对称加密算法，做为机密被保护了起来……

发明 RSA 算法的三个神人

为什么 RSA 算法会成为经典

对称加密与非对称加密

大约用时：（15 mins）

下一部分：RSA 算法原理

对称加密：凯撒密码

对称加密：雍正的折匣

所谓对称加密：

对称的是信息传递双方的『**加解密信息**』
需要保护的也是『**加解密信息**』

非对称加密举例

非对称加密举例

非对称加密举例

非对称加密举例

艾斯，听好：193

想要发送：123

非对称加密举例

想要发送：123

非对称加密举例

想要发送：123

啊，路飞实际要说：123

非对称加密举例

想要发送：123

啊，路飞实际要说：123

你俩搞什么？

一万匹……

非对称加密举例

193 * 11 = 2123
路飞想说的是 123

想要发送：123

你俩搞什么?

一万匹……

所谓非对称加密：

非对称的是信息传递双方的『**加解密信息**』
需要保护的是『**解密信息**』
所以，可以公开『**加密信息**』

公开密钥加密算法

RSA 算法过程

大约用时： （25 mins）

下一部分：RSA 算法证明

如何做制造钥匙?

『铁皮』如何变『钥匙』

第一步：选择两块上好的『铁皮』

$$N = P * Q$$

『铁皮』如何变『钥匙』

第二步：做出『钥匙』的模具

$$N = P * Q$$

$$\Phi(N) = (P - 1) * (Q - 1)$$

『铁皮』如何变『钥匙』

第三步：随便做一把『加密』的『钥匙』

$$N = P * Q$$

$$\Phi(N) = (P - 1) * (Q - 1)$$

选择 e 与 $\Phi(N)$ 互质即可

『铁皮』如何变『钥匙』

第四步：根据『加密钥匙』精心设计一把『解密钥匙』

$$N = P * Q$$

$$\Phi(N) = (P - 1) * (Q - 1)$$

选择 e 与 $\Phi(N)$ 互质即可

$$e * d \equiv 1 \pmod{\Phi(N)}$$

『铁皮』如何变『钥匙』

第五步：打包『加密钥匙』和『解密钥匙』

$$N = P * Q$$

$$\Phi(N) = (P - 1) * (Q - 1)$$

选择 e 与 $\Phi(N)$ 互质即可

$$e * d \equiv 1 \pmod{\Phi(N)}$$

『加密钥匙』：(e, N)

『解密钥匙』：(d, N)

如何做使用钥匙?

如何使用两把『钥匙』

第一步：加密人使用『加密钥匙』(e, N)

加密过程：$M^e \% N = C$

如何使用两把『钥匙』

第一步：收信息的人使用『解密钥匙』(d, N)

加密过程：$M^e \% N = C$

解密过程：$C^d \% N = M$

非对称加密的好处：

被加密的方法和信息都可以随意被窃取，
反正你没有**解密方法**

RSA 算法证明

大约用时： （10 mins）

下一部分：经典面试题刷题专项环节

RSA算法证明

加密过程：$M^e \% N = C$

解密过程：$C^d \% N = M$

经典面试题刷题专项环节

大约用时：（120 mins）

下一部分：大家晚安

问题板书

每天都想干翻这个世界
到头来，被世界干的服服帖帖

大家晚安
--船长