7. 数字签名

7.1 已知消息攻击的存在性伪造：

Oscar 向 Alice 发送的信息 x_1, x_2，让 Alice 对 x_1, x_2 签名 $y_1 = x_1^a \bmod n$，$y_2 = x_2^a \bmod n$

则 Oscar 计算 $y = y_1 y_2 = (x_1 x_2)^a \bmod n$

伪造 (x_1, x_2) 消息的签名 y.

选择消息攻击的选择性伪造：

Oscar 有消息 x 想希望获得 Alice 的签名，将 x 分解为 $x = x_1 x_2 \bmod n$.

将 x_1, x_2 分别发送给 Alice 签名，得 y_1, y_2. 则计算得 x 的签名 $y = y_1 y_2 \bmod n = (x_1 x_2)^a \bmod n$

$= x^a \bmod n$

伪造 Alice 对 x 消息的签名.

唯密钥攻击的存在性伪造：

Oscar 已知加密指数 b，Oscar 对任意签名 y 计算 $y^b \bmod n = x^{ab} \bmod n = x$,

得到伪造明文 x 为签名 y.