沟通的艺术

现代密码学的极简介绍

毛昕渝 2021/11/15

隐私与信任

现代密码学在做什么?

隐私

私密通信问题

- Alice 和 Bob 如何在公共信道上实现私密的通信?
- 对称版本：Alice和Bob可以事先共享一些信息

百方富翁问题 （Yao 82）

Two millionaires wish to know who is richer; however, they do not want to find out inadvertently any additional information about each other's wealth. How can they carry out such a conversation?

姚期智
2000年图灵奖得主

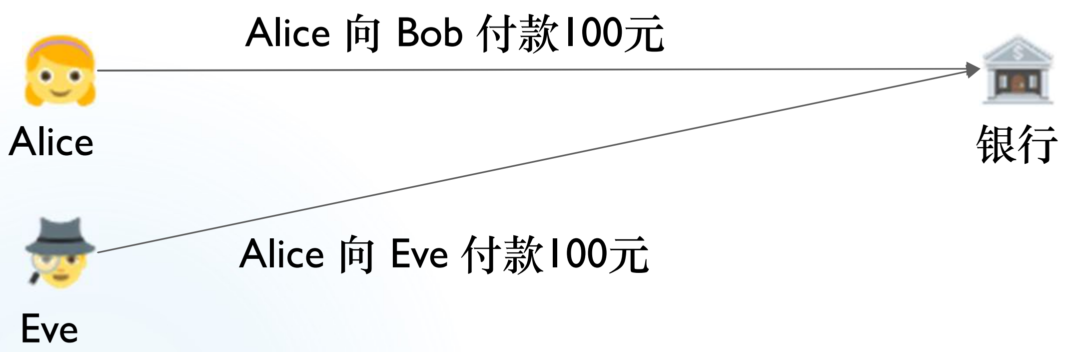
多方安全计算 Secure Multi-party Computation (SMC) Yao 86

x_1　x_2　…　x_n

计算$f(x_1, \ldots, x_n)$，并且每个人在此过程中不能知道别人的输入的任何信息。

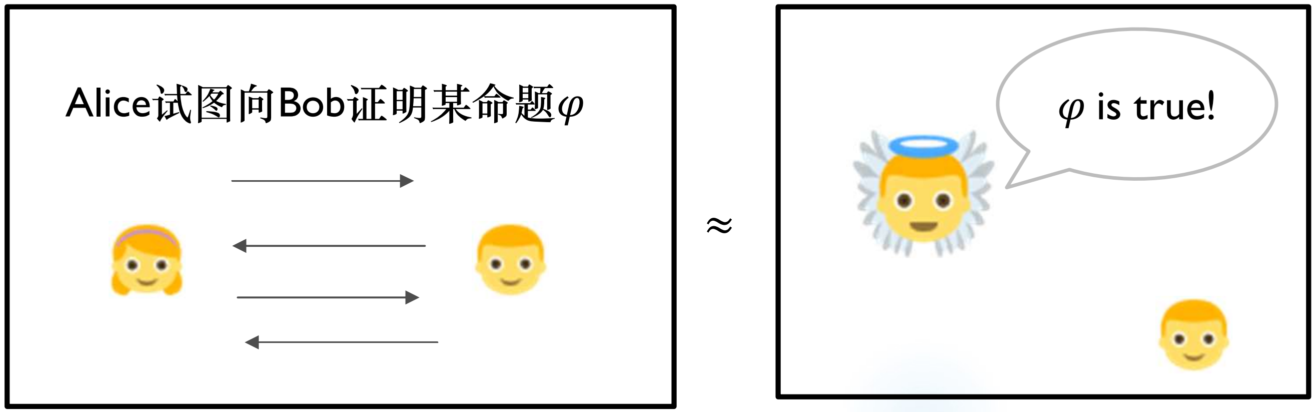
信任

消息认证 / 电子签名



如何让消息无法被伪造?
如何证明“我是Alice”?

零知识证明

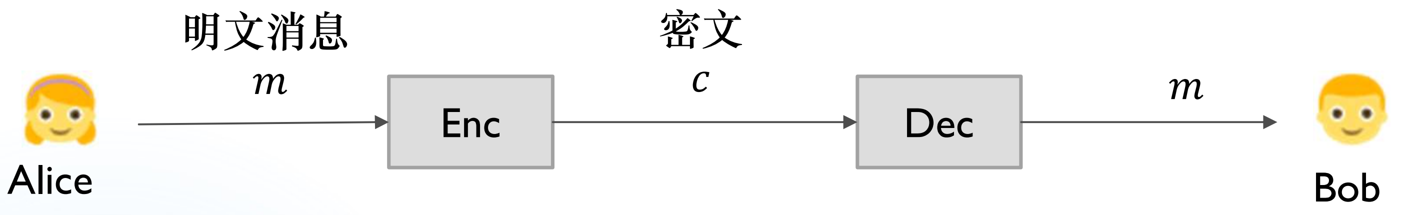


如何定义一个问题？

以对称加密为例

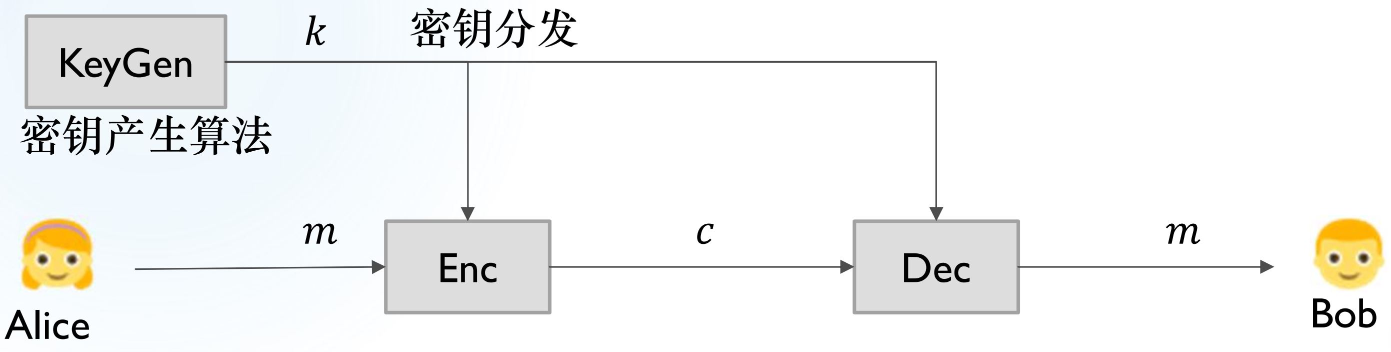
对称加密方案：大致框架

假设Alice和Bob可以事先共享一些信息，如何实现私密通信?



柯克霍夫原则（Kerckhoff's Principle）

（加密算法）不应该是秘密，它即便落入敌人之手，也不应带来不便。



安全的定义：Enigma机安全吗?

- 密钥空间大不等于安全
- 攻击者不能——
  - 破解密钥?
  - 得到明文?
  - 得到明文的任何一个比特?
- 无论攻击者事先拥有什么信息，密文不应该泄露明文的任何额外信息。
- 如何用数学语言精确定义之?
- Goldwasser 和 Micali 在 1984年的论文 *Probabilistic Encryption* 中使用的定义框架和语言深刻地影响了后来的密码学。

Enigma 机的密钥空间很大(约 1.07×10^{23})

2012年图灵奖得主

选择明文攻击下的（不可区分）安全性 IND-CPA 安全性

选择明文攻击 Chosen-Plaintext Attack

敌手可以选择一些明文，获得它们加密后的密文。

$\mathcal{C}$		$\mathcal{A}$
$k \leftarrow \Pi.keyGen$	$\xleftarrow{m}$ $\xrightarrow{Enc(k,m)}$	
$b \leftarrow \{0,1\}$	$\xleftarrow{(m_0, m_1)}$	Generate m_0, m_1
$c := \Pi.Enc(m_b)$	$\xrightarrow{c}$	
	$\xleftarrow{m}$ $\xrightarrow{Enc(k,m)}$	
$\mathcal{A}$ wins iff $b = b'$	$\xleftarrow{b'}$	Guess b'

- 一个对称加密方案由三个概率多项式时间算法组成：
  $$\Pi = (KeyGen, Enc, Dec).$$

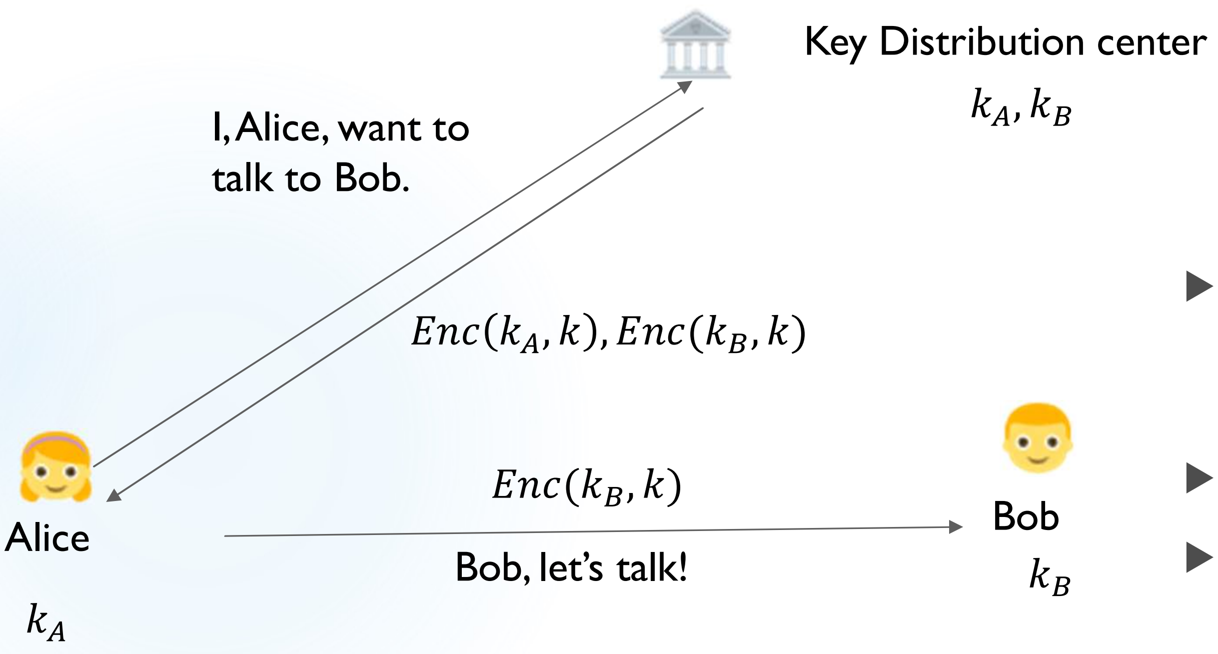
选择明文攻击下的（不可区分）安全性

如果对于所有的概率多项式时间算法$\mathcal{A}$, $\left|\Pr[\mathcal{A}\ wins] - \frac{1}{2}\right|$ 足够小，则称 Π 是 IND-CPA安全的。

Diffie-Hellman 密钥交换协议

密钥分发中心

如果我们有对称加密方案，两个从未见面的人如何进行私密通信?



没有第三方能做到吗?

- 1976年，Diffie 和 Hellman在论文 *New Directions in Cryptography* 中作出了肯定的回答。
- 这开启了公钥密码学这一全新的领域。
- 他们因此获得2015年图灵奖。

Diffie-Hellman 密钥交换协议

Alice

Bob

Let's use prime p and its ***primitive root*** g.

OK, agreed.

$k_1 \leftarrow \mathbb{Z}_p^*$

$t_1 := g^{k_1}$

t_1

t_2

$k_2 \leftarrow \mathbb{Z}_p^*$

$t_2 := g^{k_2}$

$k := t_2^{k_1}$

$k := t_1^{k_2}$

Eve

Can Eve know anything about k?

Diffie 和 Hellman证明了：在一定的假设下，k 在 Eve 的眼中与均匀随机的字符串不可区分。

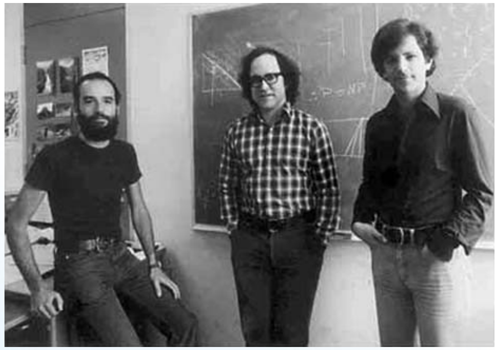
RSA加密算法

大声密谋?

Alice 和 Bob 事先不共享任何信息。

✅ 对称加密方案 + Diffie-Hellman 密钥交换协议

RSA的故事



Rivest, Shamir and Adleman 在1977年提出了RSA算法，他们因此获得 2002年图灵奖。

Clifford Cocks

英国数学家、密码学家

他在 1973 年发明了 RSA算法，但由于被认定为机密，直到1997年才为人所知。

Phil Zimmermann

- PGP的主要开发者
- 曾被美国政府指控违反武器出口限制法案 *Arms Export Control Act*

公钥加密方案

- 一个公钥加密算法 Π 由三个概率多项式时间算法组成:
  - $KeyGen(1^{\lambda})$: *输出*(pk, sk)
    - pk 称为公钥，sk称为私钥。
  - $Enc(pk, m)$
    - 输入公钥 pk和消息m，输出密文c.
  - $Dec(sk, c)$
    - 输私钥sk和密文c，输出消息m 或者输出 解密失败！

一点数学预备

- $\mathbb{Z}_n^* := \{x \in \mathbb{N}: 1 \le x \le n-1 \text{ and } \gcd(n,x) = 1\}$.
- *Fact. For every $a \in \mathbb{Z}_n^*$, there exists some $b \in \mathbb{Z}_n^*$ such that $ab \equiv 1 \bmod n$.*
  - This is guaranteed by *Bézout's theorem.*
  - b is called the **inverse** of a, denoted by a^{-1}.
- ***Euler's phi function:*** $\varphi(n) := |\mathbb{Z}_n^*|$.
  - If p is a prime, then $\varphi(p^m) = (p-1)p^{m-1}$.
  - φ *is multiplicative*: write $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, then $\varphi(n) = \varphi(p_1^{e_1})\varphi(p_2^{e_2}) \cdots \varphi(p_r^{e_r})$.
- *Theorem. For all $a \in \mathbb{Z}_n^*$, $a^{\varphi(n)} \equiv 1 \bmod n$.*
  - (Fermat's Little Theorem.) In particular, for prime p, $a^{p-1} \equiv 1 \bmod p$.
  - For every $x \in \mathbb{Z}_n^*$, $x^a \equiv x^{a \bmod \varphi(n)} \bmod n$.

RSA 加密算法

$KeyGen(1^\lambda)$:

1. Generate two λ-bit primes p, q
2. $N := pq$
3. Choose $e > 1$ such that $\gcd(e, \varphi(N)) = 1$ // $\varphi(N) = (p-1)(q-1)$
4. $d := e^{-1} \bmod \varphi(N)$
5. $pk := (N, e)$
6. $sk := (N, d)$
7. Return (pk, sk)

$Enc(pk, m)$:

1. Parse $pk =: (N, e)$
2. Return $c := m^e \bmod N$

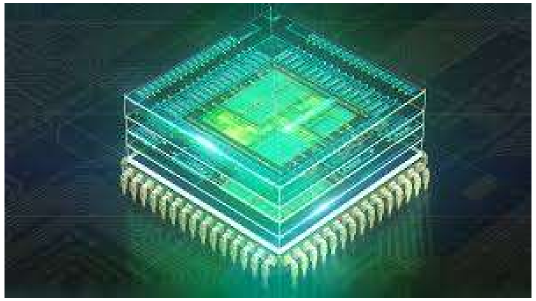
$Dec(sk, c)$:

1. Parse $sk =: (N, d)$
2. Return $m := c^d \bmod N$

- 注意 $e, d \in \mathbb{Z}_{\varphi(N)}^*$.
- 正确性: $c^d \equiv (m^e)^d \equiv m^{ed \bmod \varphi(N)} \equiv m \pmod N$.

RSA算法的安全性

- 目前尚没有不基于分解 N的攻击方法。
- 如果大数 $N = pq$ 的分解是困难的，那么RSA 是安全的
- Shor’s algorithm: 高效分解质因子的量子算法。
  - “RSA is dead.”
  - 目前进展: $91 = 7 \times 13$.



利用困难性

计算复杂性与密码学基础

现代密码学建立在明确的假设之上

- 为什么要建立在明确的假设之上?
  - 没有困难性假设就没有安全性可言
    - 在 P = NP 的世界里，密码学不复存在
  - 假设明确之后，可以据此比较方案的优劣
  - 模块化的构造
    - 量子计算机的发展使基于RSA假设的密码学构造受到挑战，我们可以基于其他假设来构建密码学的一切。

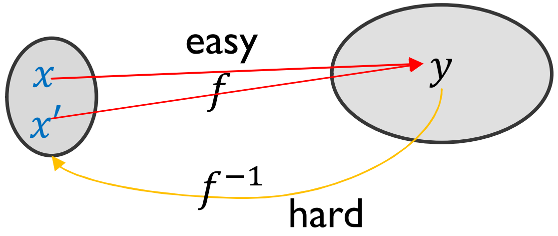
密码学的最小假设：存在单向函数

单向函数（One-way function）

如果函数$f:\{0,1\}^* \rightarrow \{0,1\}^*$ 满足如下条件，则称之为单向函数：

- （正向求值容易） f 是多项式可计算的；
- （反向求逆困难）对于任意的概率多项式算法 $\mathcal{A}$ 和多项式 p:

$$\Pr_{\substack{x\leftarrow\{0,1\}^n \\ y:=f(x)}}[\mathcal{A}(y) = x' \wedge f(x') = y] \leq \frac{1}{p(n)}.$$



假设. 存在单向函数。

如果上述假设成立，则有$\mathbf{P} \neq \mathbf{NP}$.

五个世界：我们生活在哪个世界之中？

[Impagliazzo’s five worlds]

sampNP：能高效采样的NP问题分布
distP：能高效解决的问题分布

- **Algorithmica**: P=NP.
- **Heuistica**: P≠NP 但是 sampNP⊆distP.
- **Pessiland**: sampNP ⊈ distP, 但不存在单向函数。
  - 这里的生活很困难，但我们甚至无法利用困难性来构建密码学。
  - 真是个糟糕的世界！
- **Minicrypt:** 单向函数存在，但NP中很有结构的问题都在P中.
  - 密码学理论上存在，但几乎没有实用价值。
- **Cryptomania:** 有些很有结构的问题在平均意义下是困难的。
  - 密码学的理想世界。
  - 或许我们就生活在这里☺

Thanks for listening. ☺