西安交通大學
XI'AN JIAOTONG UNIVERSITY

密码学 AUTO712705

第 4 章：消息认证码
Message Authentication Codes

赵俊舟

西安交通大学网安学院

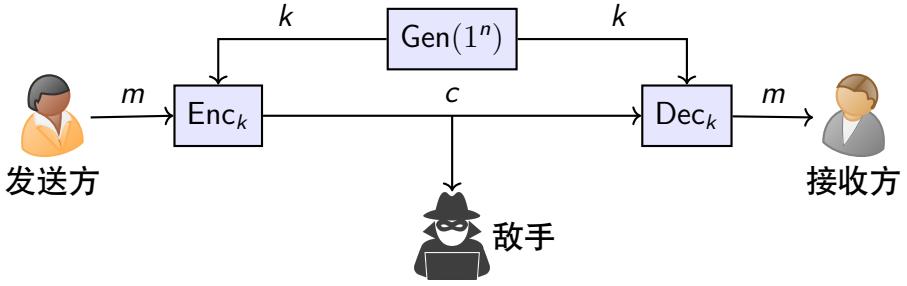
junzhou.zhao@xjtu.edu.cn

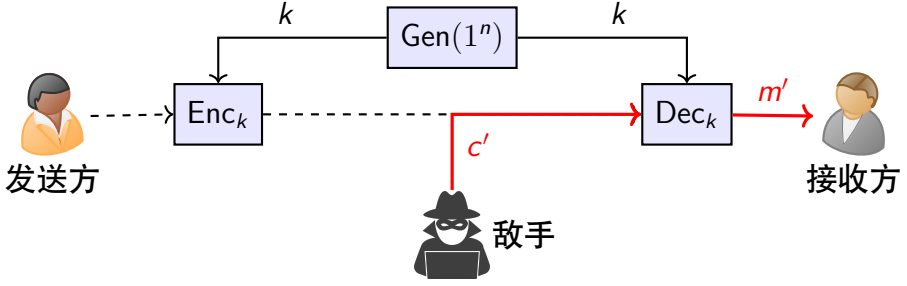
2025 年 12 月 20 日

目录

目录

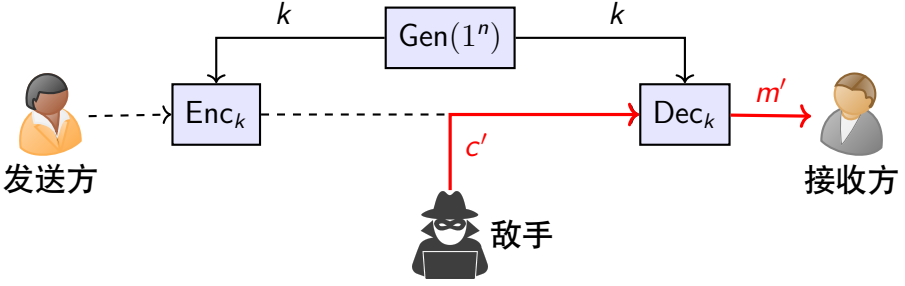
消息保密与消息认证


k
Gen(1^n)
k
m
Enc_k
c
Dec_k
m
发送方
接收方
敌手


k
Gen(1^n)
k
Enc_k
Dec_k
m′
c′
发送方
接收方
敌手

消息保密与消息认证

- 私钥加密可以保证消息的保密传输，但无法防止敌手主动作恶：伪造消息和篡改消息。
- 伪造消息：银行收到一条伪造的转账请求，要求从账户 A 转账 1 万元到账户 B。
- 篡改消息：账户 A 要求银行转账 1 万元到账户 B，消息被敌手修改为转账 10 万元到账户 C。



网络通信环境中的攻击

- **泄密**：将消息透露给没有密钥的第三方
- **传输分析**：分析双方通信模式

消息保密

- **消息伪装**：欺诈源向网络中插入一条消息
- **身份伪装**：发送方伪装为其他身份
- **内容篡改**：对消息内容的修改
- **顺序篡改**：对消息顺序的修改
- **计时篡改**：对消息的延时和重放

消息认证

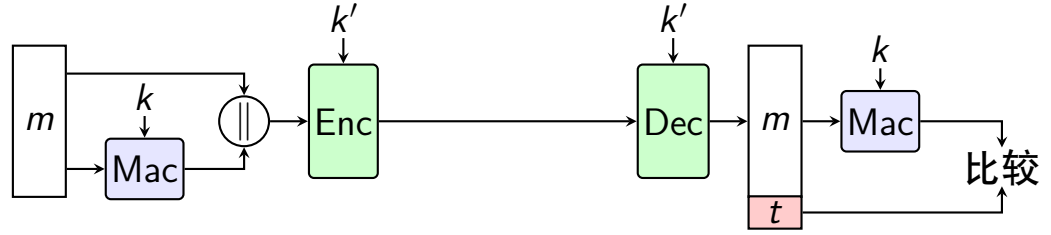
- **信源抵赖**：发送方否认发送过某消息
- **信宿抵赖**：接收方否认接收过某消息

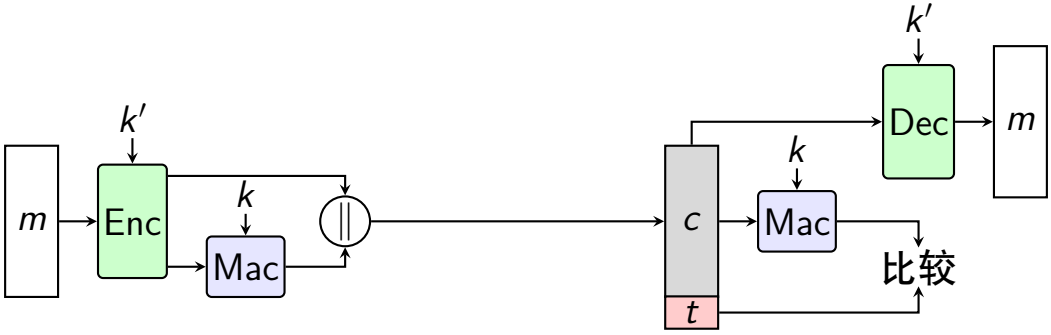
数字签名 + 其他手段

消息认证码（Message Authentication Code）

- 消息认证的作用是实现通信双方对消息完整性的验证，防止敌手篡改或伪造消息。
- 通信双方都持有密钥 k；
- 发送方在发送消息 m 前，计算消息 m 的消息认证码，即 $t = \mathrm{Mac}_k(m)$，然后将 (m, t) 作为报文整体发送给接收方；
- 接收方收到报文 (m, t) 后，使用一个验证算法 Vrfy 对报文进行验证。

消息认证码的其他工作模式





消息认证码的定义

定义 (消息认证码)

消息认证码（MAC）由三个 PPT 算法 (Gen, Mac, Vrfy) 组成，满足以下条件：

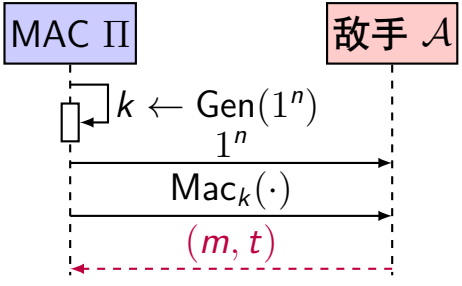
- 密钥生成函数 Gen: 输入安全参数 1^n，输出密钥 k 且 $|k| \geq n$;
- 消息认证码生成函数 Mac: 输入密钥 k 和消息 $m \in \{0,1\}^*$，输出消息认证码 $t \leftarrow \mathsf{Mac}_k(m)$;
- 验证函数 Vrfy: 输入密钥 k，消息 m 和消息认证码 t，输出比特 $b = \mathsf{Vrfy}_k(m, t)$。

- 正确性要求：$\mathsf{Vrfy}_k(m, \mathsf{Mac}_k(m)) = 1$.

目录

安全性定义

- 安全的消息认证码体制不应让敌手能够对一条新发送的消息生成正确的消息认证码。
- 选择消息攻击假设：敌手可以观察 (m, t) 对，并欺骗发送方生成 m' 的消息认证码 t，即具有选择消息攻击能力。



- 敌手具有神谕 $\mathsf{Mac}_k(\cdot)$，可以得到任意消息的消息认证码。
- 如果敌手能生成消息 m 的消息认证码 t 且之前未对 m 使用过神谕，则称敌手攻击成功，记为

$$\text{Mac-forge}_{\mathcal{A},\Pi}(n) = 1$$

- 如果对任意 PPT 敌手，都存在可忽略函数 negl，满足

$$\Pr[\text{Mac-forge}_{\mathcal{A},\Pi}(n) = 1] \leq \text{negl}(n)$$

称消息认证码 $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ 是安全的。

其他威胁：重放攻击

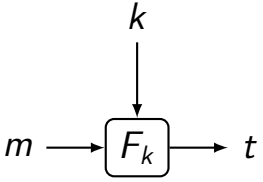
- Alice 向银行发送一个转账请求，请求向 Bob 转账 1000 元。
- 如果消息认证码是安全的，那么可以防止敌手将转账金额修改为 10000 元，并且得到正确的消息认证码。
- 但敌手可以截获 Alice 发送的消息及其验证码 (m, t)，并且将 (m, t) 重复发送 10 次，这等效于让 Alice 转账了 10000 元。
- 消息认证码本身不能防止这样的重放攻击，解决手段依赖于给消息加上时间戳或者序列号。

目录

定长消息认证码的构建

设计 (定长消息认证码)

- 令 F 为一个伪随机函数;
- Mac: 输入密钥 $k \in \{0,1\}^n$ 和消息 $m \in \{0,1\}^n$，输出消息认证码 $t = F_k(m)$;
- Vrfy: 输入密钥 $k \in \{0,1\}^n$，消息 $m \in \{0,1\}^n$ 和消息认证码 $t \in \{0,1\}^n$，当且仅当 $t = F_k(m)$ 时输出 1。

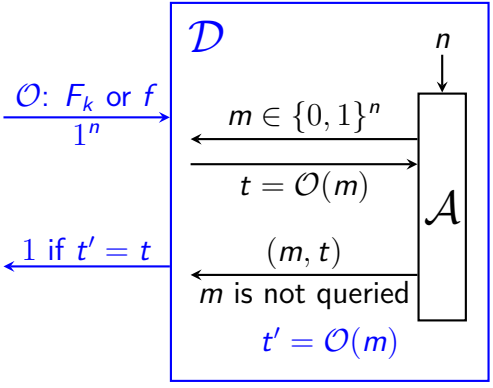


定理 (安全性)

当 F 是伪随机函数时，上述方法构建的消息认证码是安全的。

证明思路

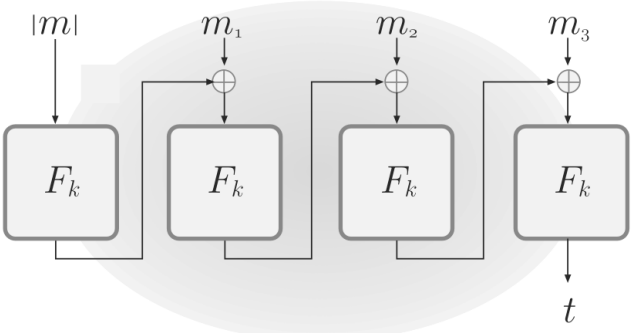
- 如果敌手 $\mathcal{A}$ 可以攻破消息认证码 Π，那么可以用 $\mathcal{A}$ 构造一个区分器 $\mathcal{D}$，用来区分 F_k 是伪随机函数还是随机函数 f。
- 但是实际中区分器 $\mathcal{D}$ 无法区分伪随机函数和随机函数，所以敌手 $\mathcal{A}$ 无法攻破消息认证码 Π。



- 敌手 $\mathcal{A}$ 作为子程序被区分器 D 调用；
- 敌手 $\mathcal{A}$ 可以查询任意消息的认证码；
- 敌手 $\mathcal{A}$ 最后输出一个新消息及其认证码 (m, t) 且 m 未被查询过；
- 区分器计算 $t' = \mathcal{O}(m)$，当 $t' = t$ 时输出 1 否则输出 0。

任意长消息认证码的构建：CBC-MAC

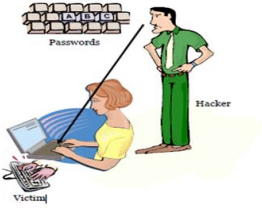
- 当消息长度大于 n 时怎么办？
- 可以基于分组密码的密文分组链接工作模式设计 CBC-MAC。
- 缺点：计算效率随消息长度增长而降低。
- 其他方法：GMAC、Poly1305 等



目录

肩窥攻击与双因素认证

- 肩窥攻击（Shoulder Surfing Attack）



- 双因素认证（Two-Factor Authentication）

- A user logs into a service using something they know (e.g., a password) and something they have (e.g., a phone).
- Timed One-Time Password (TOTP): $t = \mathrm{Mac}_k(s)$ where s is current time and rounded into 30 seconds.

小结

1. 消息认证码的定义
2. 消息认证码的安全性
3. 消息认证码的构建
4. 消息认证码的其他应用