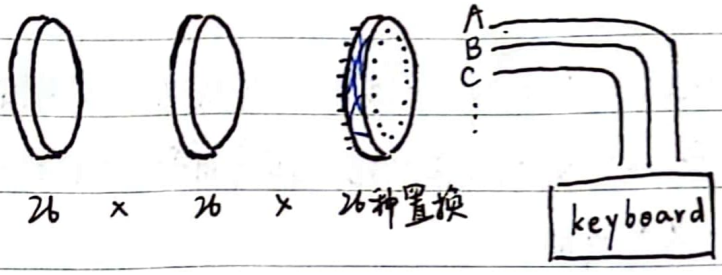
2024.09.11

cryptograhy：开始用于军事领域，从二战后开始发展。历史上：cipher

- Caesar cipher：每个字母后移三位
- shift cipher：每个字母后移 key 位。key $\in \{0,1,2,\cdots,25\}$
- substitution cipher：用一个字母表到字母表的双射作为 key　$f:\{A,B,\cdots,Z\}\to\{A,B,\cdots,Z\}$
- Vigenere cipher：key：$f_1,f_2,f_3,\cdots,f_k$ 多个双射。

  破解方法：猜长度 (k)。按猜的长度统计词频，看是否与英语词频相吻合。
- Enigma：类似 Vigener cipher，但 key：$f_1,f_2,\cdots,f_{26^3}$

结构：



key：pos_1,pos_2,pos_3。

破解方法：暴力枚举 pos_1,pos_2,pos_3。

一般地，一个加密 Scheme：(M,C,K,Gen,Enc,Dec)

明文空间 Plaintext Space：M　　密钥生成函数 Key Generation：Gen：$\to K$

密文空间 Ciphertext Space：C　　加密函数 Encryption：Enc：$K\times M\to C$

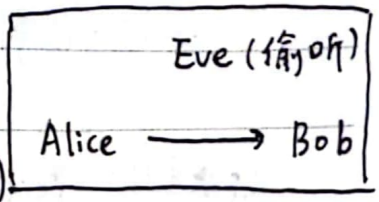
密钥空间 Key Space：K　　解密函数 Decryption：Dec：$K\times C\to M$。

- 正确性 Correctness：$\forall k,m.\ Dec(k,Enc(k,m))=m$。

Definition：基于 Assumption（例如大素数相乘难分解），得到安全性的 Proof

安全性：- Key Recovery Attack

- Message Recovery Attack
- "Eve learns nothing useful"（Semantically secure）



定义：$f:M\to\{0,1\}$。对 $\forall$ 分布 D_M：$\forall eve.\ Pr[eve(Enc(k,m))=f(m)]=Pr[s(\cdots)=f(m)]$

$(k\leftarrow Gen,\ m\leftarrow D_M)$　$(\forall f)$。

不够严谨. 考虑有信息泄露. $g: M \to T$. 要有

定义1'. 对 $\forall D, m, g, eve, f, \exists S$. $Pr[Eve(Enc(k,m), g(m)) = f(m)] = Pr[S(g(m)) = f(m)]$

. 该定义是否比上一个定义更强?

其它定义: Distinguisher: "Can not tell the ciphertexts of two distinct messages".

定义2. $\forall D, m_0, m_1$. $Pr[D(Enc(k,m_0)) \to 0] = Pr[D(Enc(k,m_1)) \to 0]$.

$$\Pr_{b \leftarrow \{0,1\}}[D(Enc(k,m_b)) = b] = \frac{1}{2}$$

Perfect Secrecy:

定义3. $\forall m_0, m_1, c$. $\Pr_k[Enc(k,m_0) = c] = \Pr_k[Enc(k,m_1) = c]$.

定义2 ⇒ 定义3: 让D为"若密文为c则输出0. 否则输出1"即可.

定义3 ⇒ 定义2: 得到任意一个值的概率相等 ⇒ D判别出来的概率相等.

这3个定义是等价的.

不一定是最好的安全性. 但在Eve只能读取一次. 不知道任何key等条件下. 是最好的安全性

. 一种符合该安全性的加密方式: One-time Pad

$M: \{0,1\}^n$. $C: \{0,1\}^n$. $K: \{0,1\}^n$. Gen: 随机采样

$Enc(k,m) = k \oplus m$ (按位xor). $Dec(k,c) = k \oplus c$

正确性显然. 安全性: $\Pr_k[Enc(k,m_0) = c] = \Pr_k[Enc(k,m_1) = c] = \frac{1}{2^n}$. ✓

One-time Pad 的缺问题: 密钥空间和明文空间一样大.

能否让 $|K| < |M|$? 在该定义下不可以.

攻击者可枚举密钥. 得到的可能的明文数量 < 实际的明文数量.

解决方法: Perfect Secure → Statistical Secure / δ-Secure.

$\Pr_{b \leftarrow \{0,1\}}[D(Enc(K,m_b)) = b] \le \frac{1}{2} + \delta$. 但$\delta$-Secure下 $|K|$ 仍不能比 $|M|$ 小太多

★ · computational secure / (τ, δ)-secure

更改定义. e.g. 在 Distinguisher 中, D 的运行时间 $\leq \tau$

一般不用具体的时间. 用类似 (poly, negl)

λ - security parameter ($\approx$ key length).

- $K_1, K_2, \cdots, K_\lambda$
- $M = \{0,1\}^*$ (任意有限长的 0-1 串).
- $C = \{0,1\}^*$
- $Gen(1^\lambda) \to K_\lambda$
- $Enc: K \times M \to C$
- $Dec: K \times C \to M$

} 要求是 poly 的

$poly(\lambda) = \bigcup_k O(\lambda^k)$.

$negl(\lambda) = \bigcap_k O(\frac{1}{\lambda^k})$ (趋于 0 的速度比任何多项式分之一都快) e.g. $e^{-\lambda}$.

Definition:

- 正确性 Correctness
- 安全性 Security
  - Eveadropper (Passive) / Active !
  - Single message / Multi message !
  - Perfect / Statistical / Computational (poly time adversary, negl advantage)

定义1与定义3的等价性: 3⇒1. 构造 S: 随机采样一个 c. 输出 eve(c) 即可.

1⇒2. 令 $D_M = \{m_0, m_1\}$ 上的均匀分布. $f(m_0)=0$. $f(m_1)=1$ 即可.

1⇒1'. 给定 $g(m)$ 时. 把 1 定义中的 D_M 换成 D_M conditional on g 即可.

- 考虑 one-time pad 中，用 G(seed) 替代 key，什么情况下是安全的？
  - 无法根据一些位猜出下一位 (computational 意义下).
  or - 无法区分 key 是用种子生成的还是随机生成的