





无密钥信息伪装系统

定义

对一个五元组 Σ =〈C, M, C', D, E〉, 其中C是所有可能 载体的集合,M是所有可能秘密消息的集合,C'是所有可能伪装 对象的集合。E: C×M→C'是嵌入函数,D: C'→M是提取函数, 若满足性质: 对所有m∈M和c∈C, 恒有: D(E(c, m))=m, 则称 该五元组为无密钥信息伪装系统。





相似性函数

载体对象和伪装对象在感觉上不可区分,如何度量?

定义

设C是一个非空集合,一个函数 $sim: C^2 \rightarrow (-\infty,1)$, 对 $x, y \in C$,若满足:

$$sim(x,y) \begin{cases}
=1 & x = y \\
<1 & x \neq y
\end{cases}$$

则sim称为C上的相似性函数 相似度应尽可能接近1





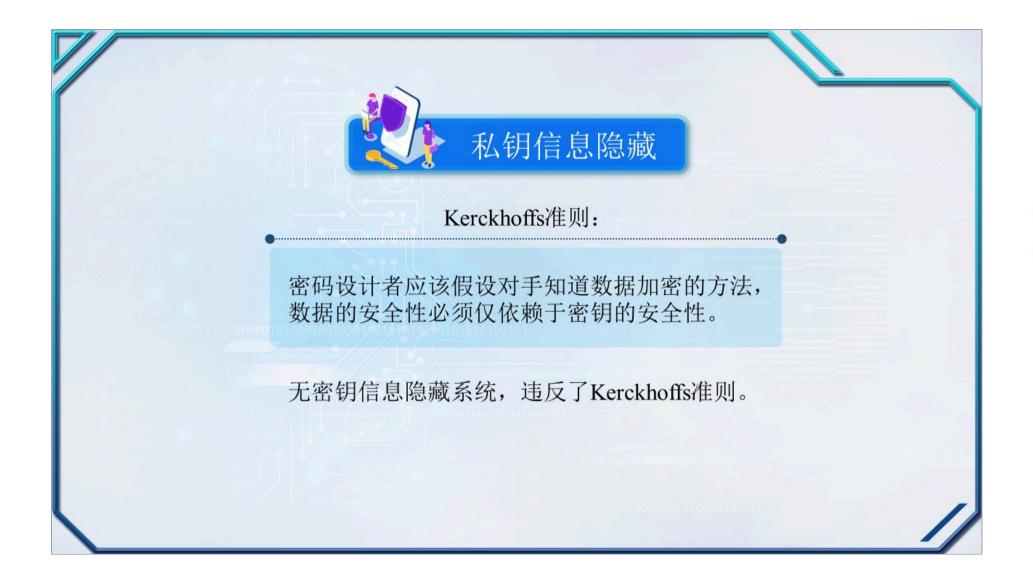
载体的选择

不同的嵌入算法, 对载体的影响不同。

选择最合适的载体,使得信息嵌入后影响最小,即载体对象与伪装对象的相似度最大。

$$c = Max \atop x \in C$$
 sim $(x, E(x, m))$









私钥信息隐藏

定义

对一个六元组 Σ =〈C,M,K,C', D_K , E_K 〉,其中C是所有可能载体的集合,M是所有可能秘密消息的集合,K是所有可能密钥的集合, E_K : C×M×K→C'是嵌入函数, D_K : C'×K→M是提取函数,若满足性质: 对所有m∈M,c∈C和k∈K,恒有: D_K (E_K (c,m,k),k)=m,则称该六元组为私钥信息隐藏系统。

私钥的传递:

密钥交换协议





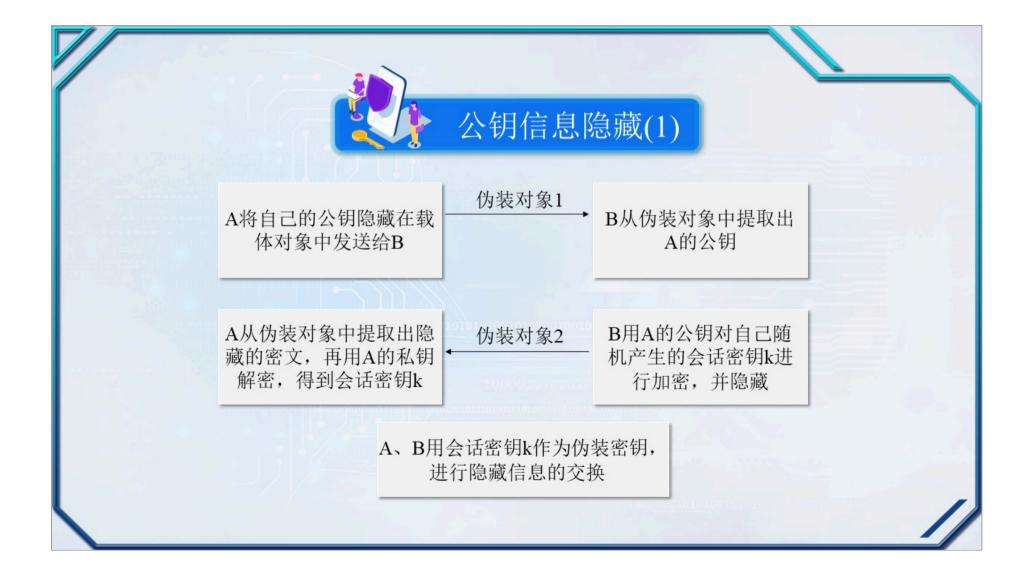
公钥信息隐藏

- ※ 类似于公钥密码。
- 通信各方使用约定的公钥体制,各自产生自己的公开钥和秘密钥,将 公开钥存储在一个公开的数据库中,通信各方可以随时取用,秘密钥 由通信各方自己保存,不予公开。

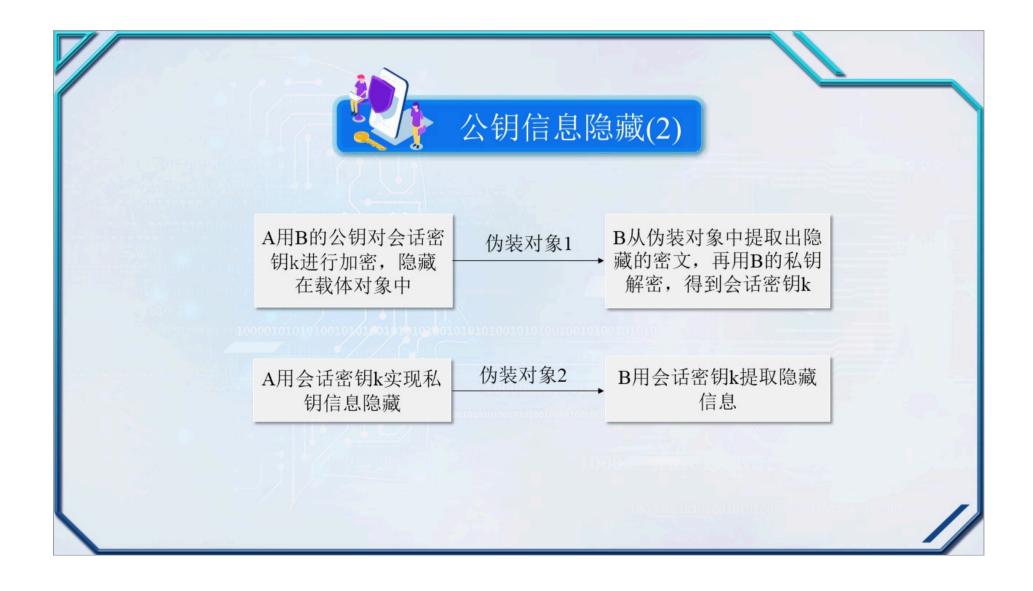
- 11/15页 -

- ※ 公钥用于传递会话密钥。
- ※ 会话密钥用来作为伪装密钥。









- 13/15页 -



