通 信 安 全

L1—通信安全基础

- 教师：崔爱娇

- 编号：ELEC3019
- 学时：32学时

概 要

通信安全基础

- 信息与通信
- 安全与通信
- 信息安全属性
- 核心

概 要

通信安全基础

- 信息与通信
- 安全与通信
- 信息安全属性
- 核心

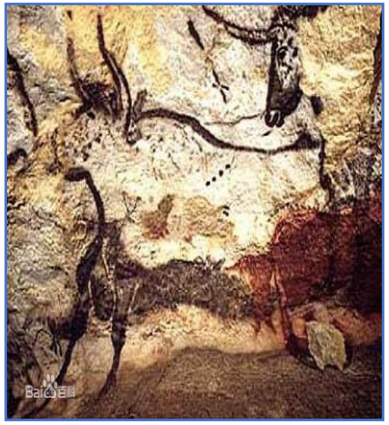
信息与通信

信息奠基人香农认为： 信息是用来消除随机不确定性的东西。[1]

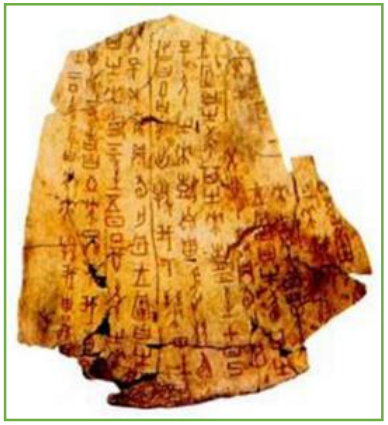
通信，指人与人或人与自然之间通过某种行为或媒介进行的信息交流与传递。[2]

语言：传递信息的声音

结绳记事



山洞壁画



甲骨文

[1] Claud Shannon, “A mathematical theory of communication,” in *Bell System Technical Journal*, 1948.

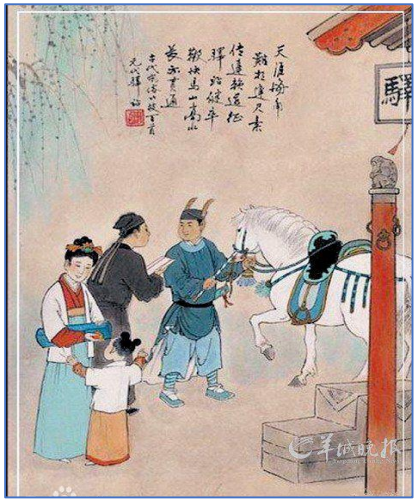
[2] https://baike.baidu.com/item/%E9%80%9A%E4%BF%A1/300982?fr=aladdin

古代的通信

烽火

击鼓鸣金

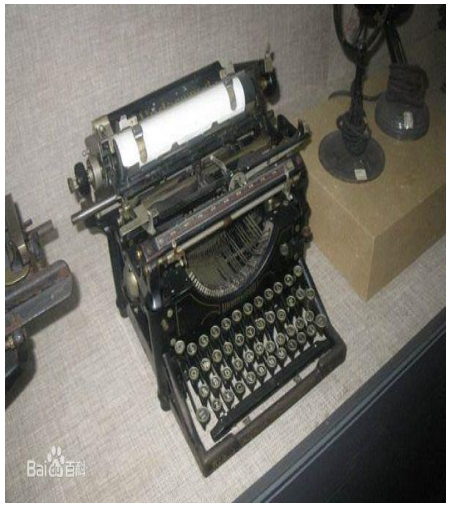
鸿雁传书



驿站

缺点？　如何远距离、高速传输？？

近代的通信



电报机
1837年
美国人
摩尔斯

电话机
1875年
美国人
贝尔

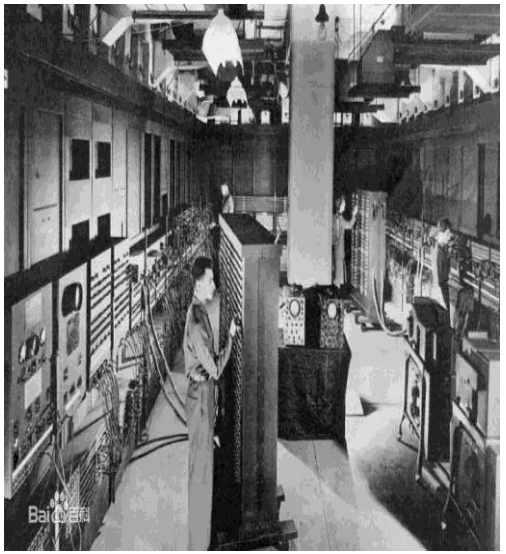
无线电接收机
1895年
俄国人波波夫
意大利人马可尼

电影
1895年
法国
卢米埃兄弟

近代的通信

收音机
1920年代

电视
1925年
英国人
贝尔德



计算机
1946年
美国
军方ENIAC

现代的通信

ARPANET
1969年
美国军方

互联网
1983年
美国
军网 民网

信息高速公路
1993年
美国
整合电脑、电视、电话

概 要

通信安全基础

- 信息与通信
- 安全与通信
- 信息安全属性
- 核心

古代的“安全”

阴符
中国周朝
长短不同的竹片
三寸表示溃败
四寸表示将领阵亡
五寸表示请求增援
六寸表示坚守

阴书
宋代
分开，编码

以矾书帛，入水方见
宋代
裹蜡 入腹

古代的“安全”

头皮写字
古希腊

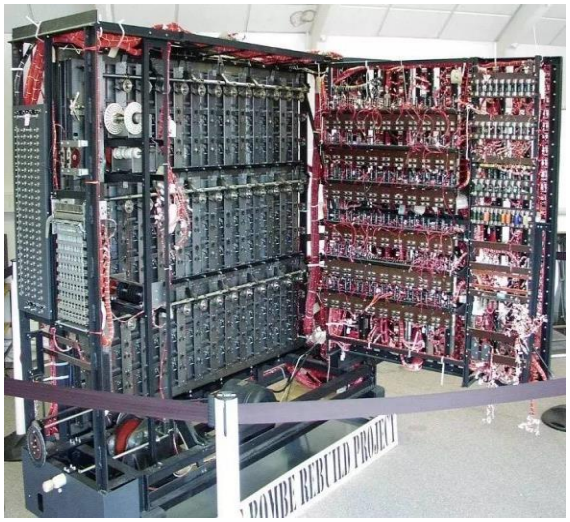
隐写术

杰弗逊圆盘
美国总统
36片，26个字母

近代的“安全”

微缩照片
二战
德军

ENIGMA机器
二战
德军
10^{16}
3亿年



“炸弹”密码破解机
图灵
英国

概 要

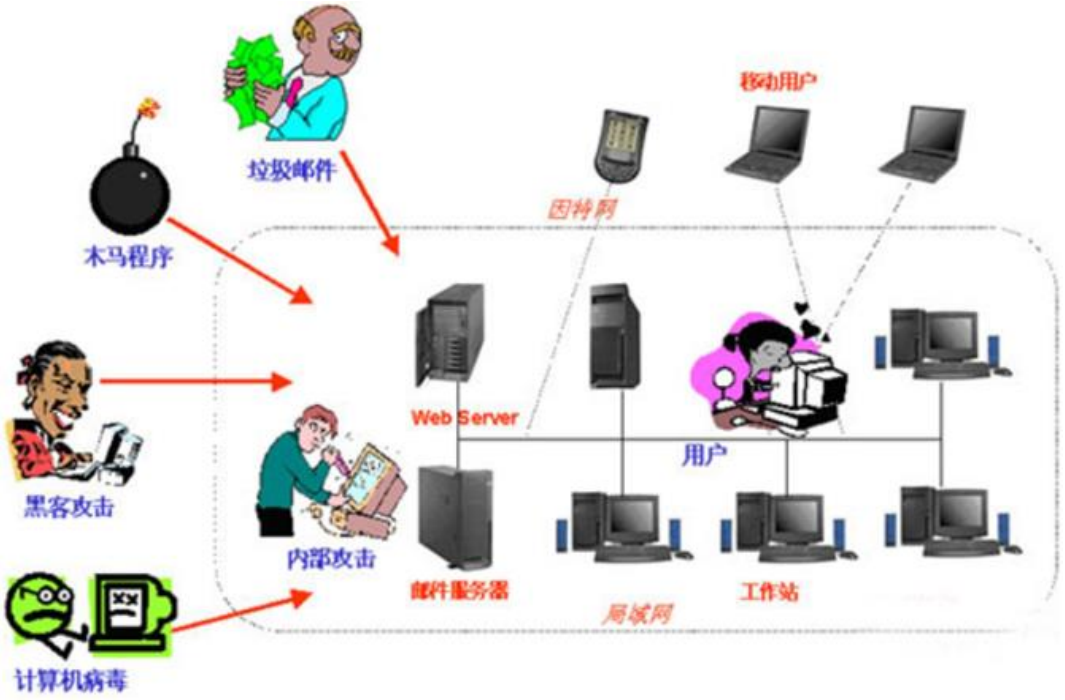
通信安全基础

- 信息与通信
- 安全与通信
- 信息安全属性
- 核心

信息安全

安全：没有受到威胁、没有危险、危害、损失。

信息安全：信息进行安全的传输和存储的理论、技术、方法和规范等的总和。

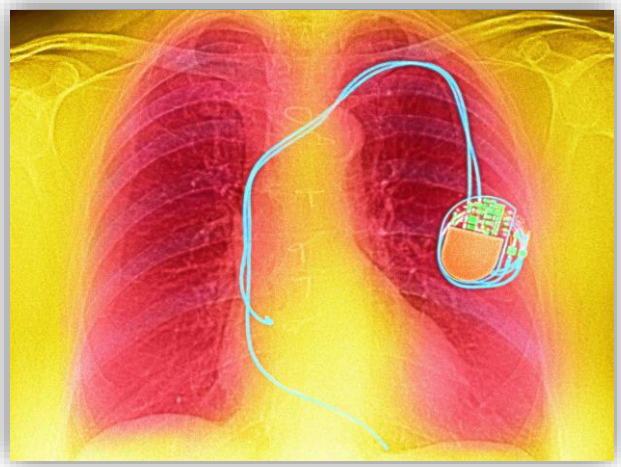


信息安全

2017年4月-永恒之蓝

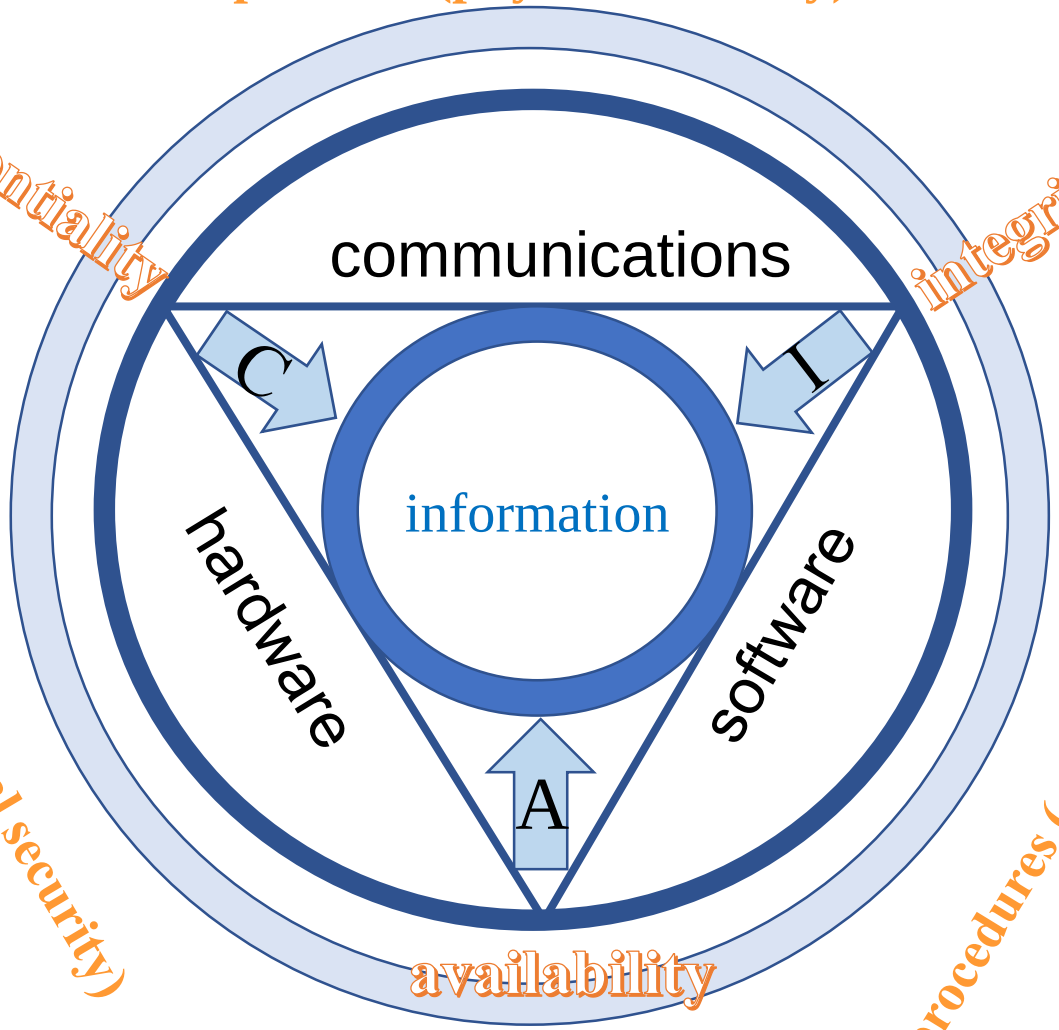
2010年7月28日--ATM机吐钞票

2012年--胰岛素泵的致命缺陷



2013年—心脏起搏器，遥控杀人
2016年—入侵植入式医疗器械

信息安全属性



指只有授权用户可以获取信息

指信息在输入和传输的过程中，不被非法授权修改和破坏，保证数据的一致性

指保证合法用户对信息和资源的使用不会被不正当地拒绝

概 要

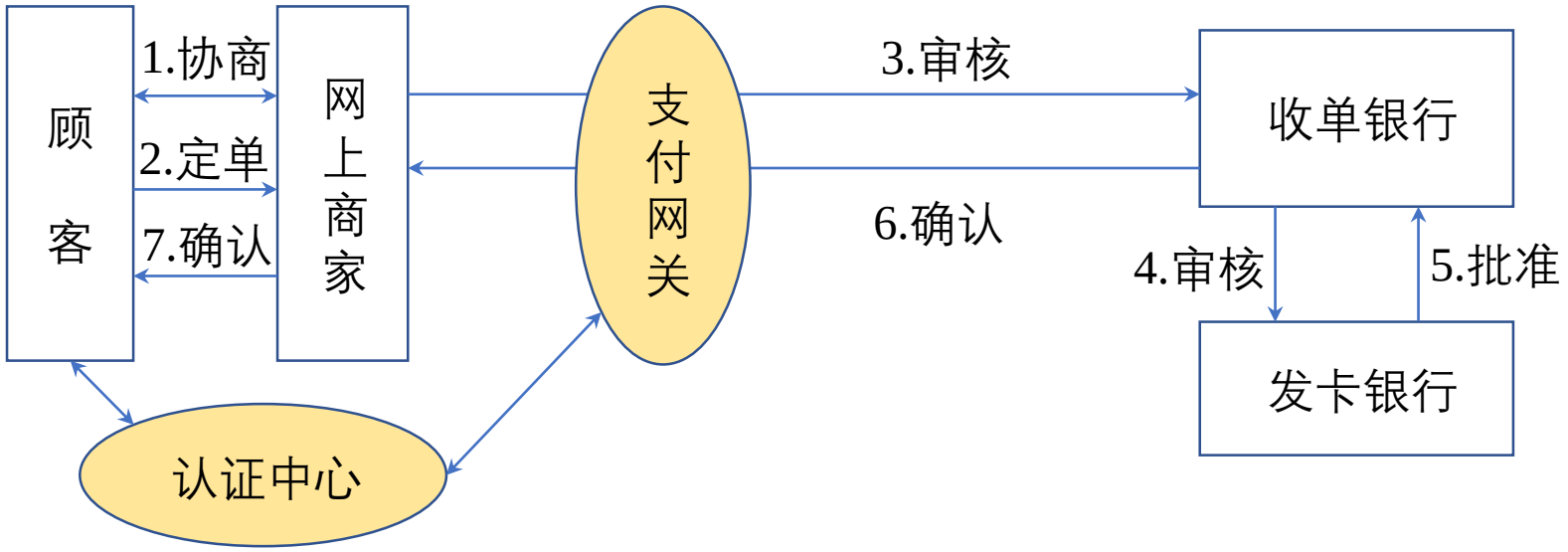
通信安全基础

- 信息与通信
- 安全与通信
- 信息安全属性
- 核心

核 心

密码是一种用来混淆的技术，使用者希望将正常的（可识别的）信息转变为无法识别的信息。但这种无法识别的信息部分是可以再加工并恢复和破解的。

安全协议是建立在密码体制基础上的一种交互通信协议，它运用密码算法和协议逻辑来实现认证和密钥分配等目标。



作 业

1. 描述一个生活中或设想中的需要信息安全的场景；

2.给出自己的安全方案；

举例：银行卡网络交易，输入密码。

3. 亚历山大贝尔生平读后感