网络工程与科学导论

第8章 网络安全基础

高峰
计算机科学与技术学院
武汉科技大学
feng.gao86@wust.edu.cn

第8章　网络安全基础

- 8.0 引言
- 8.1 密码学
- 8.2 对称密钥算法
- 8.3 公开密钥算法
- 8.4 数字签名
- 8.5 通信与WEB安全

引言 —— 历史上的著名计算机病毒

CIH 病毒

- CIH病毒是一种能够破坏计算机系统硬件的恶性病毒。这个病毒产自台湾，集嘉通讯公司（技嘉子公司）手机研发中心主任工程师陈盈豪在其于台湾大同工学院念书期间制作。最早随国际两大盗版集团贩卖的盗版光盘在欧美等地广泛传播，随后进一步通过网络传播到全世界各个角落。

熊猫烧香

- 熊猫烧香是一种恶性的计算机病毒，是一种经过多次变种的“蠕虫病毒”变种，2006年10月16日由25岁的中国湖北武汉新洲区人李俊编写，拥有感染传播功能，2007年1月初肆虐网络，它主要通过下载的档案传染，受到感染的机器文件因为被误携带间接对其它计算机程序、系统破坏严重。2013年6月病毒制造者张顺和李俊团伙同他人开设网络赌场，再次获刑。

引言 —— 2016年信息安全事件

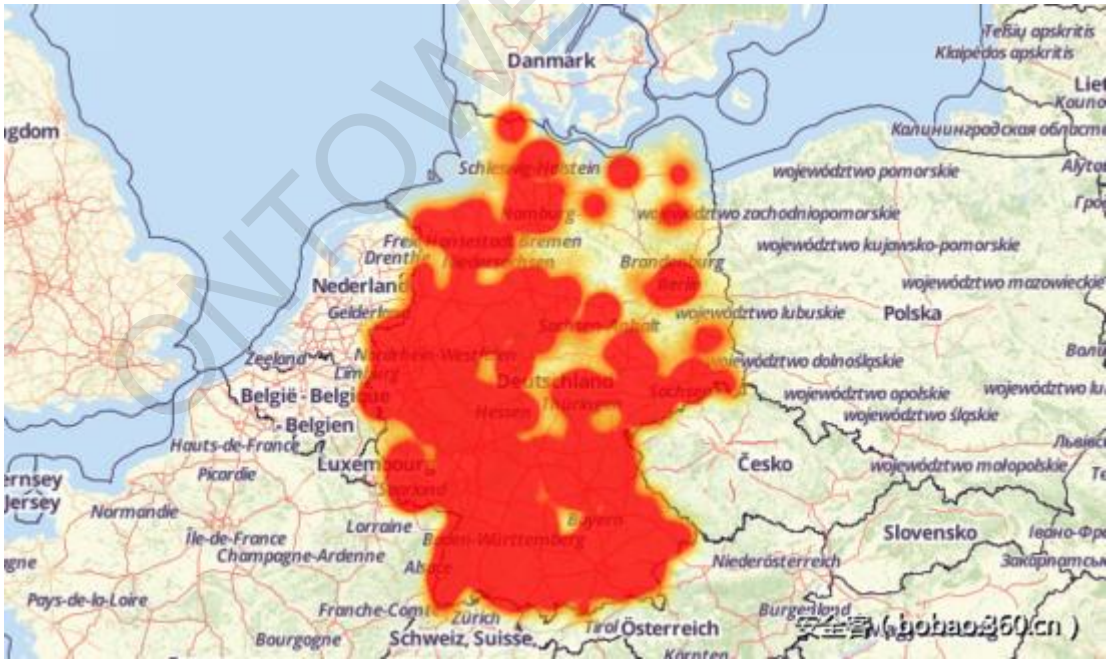
➢No.1：俄罗斯央行遭黑客攻击 3100万美元不翼而飞

- 12月，俄罗斯中央银行官员瑟乔夫证实，该行电脑系统遭到了黑客入侵，犯罪分子从银行的代理账户中窃走了20亿卢布（约合3100万美元）的资金。瑟乔夫透露，黑客是通过伪造一名用户的证书进入的这些账户。紧接着，俄罗斯第二大银行VTB再遭黑客攻击，幸运的是，银行方面的防御体系成功击退了指向其业务系统的DDoS攻击，未造成资金损失。

引言 —— 2016年信息安全事件

➢No.2：德国90万家庭断网 遭黑客蓄意入侵

- 11月，德国电信遭遇一次大范围的网络故障。2000万固定网络用户中的大约90万路由器发生故障（约4.5%），并由此导致大面积网络访问受限。德国电信进一步确认了问题是由于路由设备的维护界面被暴露在互联网上、并且互联网上正在发生针对性的攻击而导致。



引言 —— 2016年信息安全事件

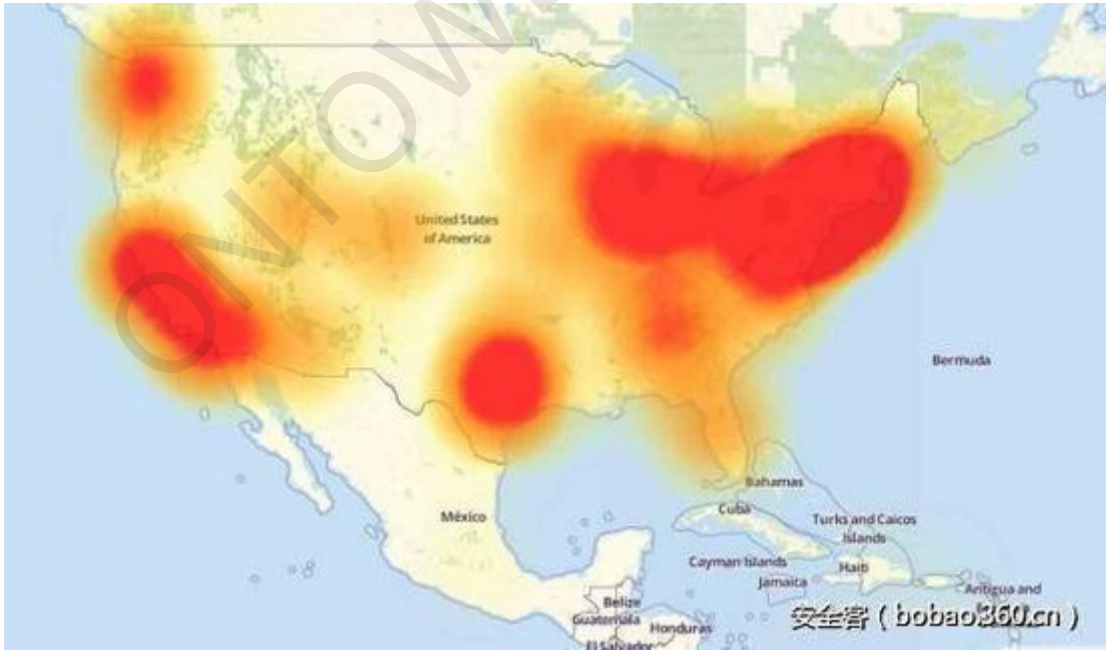
➢No.3：旧金山地铁被勒索软件攻击 乘客免费乘坐地铁

- 11月，旧金山的Municipal地的电脑票价系统遭到黑客攻击，黑客索要100比特币作为赎金。尽管旧金山地铁没有公布案件调查进展信息，但我们能从中看出这是一次恶意的黑客勒索软件攻击事件，若要恢复地铁票价系统就需要进行比特币赎金交易。旧金山地铁拒绝接受讹诈，干脆开放所有地铁闸门。

引言 —— 2016年信息安全事件

➢No.4：美国遭史上最大规模DDoS攻击、东海岸网站集体瘫痪

- 10月，恶意软件Mirai控制的僵尸网络对美国域名服务器管理服务供应商Dyn发起DDoS攻击，从而导致许多网站在美国东海岸地区宕机，如GitHub、Twitter、PayPal等，用户无法通过域名访问这些站点。



引言 —— 2016年信息安全事件

No.5：希拉里邮件门事件

- 2015年年初，邮件门事件首次被曝光，希拉里在2009年至2013年担任美国国务卿期间，违规使用私人电子邮箱和位于家中的私人服务器收发大量涉密的邮件.涉嫌违反美国《联邦档案法》，面临调查时又匆匆删除。2016年夏季，美国民主党全国委员会、筹款委员会、竞选团队被黑客组织入侵，近2万封邮件被维基解密披露。邮件显示，希拉里涉嫌抹黑竞争对手，以及可能涉嫌洗钱等财务问题。10月28日，大胖子黑客Kim Dotcom翻出了被希拉里删除的邮件，导致FBI重新开始调查希拉里邮件门事件

引言 —— 2016年信息安全事件

➢No.6：雅虎曝史上最大规模信息泄露 5亿用户资料被窃

- 9月，雅虎突然宣称其至少5亿条用户信息被黑客盗取，其中包括用户姓名、电子邮箱、电话号码、出生日期和部分登录密码。并建议所有雅虎用户及时更改密码。此次雅虎信息泄漏事件被称为史上最大规模互联网信息泄露事件，也让正在出售核心业务的雅虎再受重创。

引言 —— 2016年信息安全事件

➢No.7：美国国家安全局陷入斯诺登之后最大泄密风波

- 继斯诺登泄密风波之后，美国国家安全局（NSA）再次敲响内部威胁警钟。NSA承包商哈罗德•马丁于8月27日因窃取国安局数据被捕，马丁与曾揭露美国政府大规模监听行动的斯诺登受雇于同一家公司，马丁还被怀疑掌握了NSA的“源代码”，这些源代码通常被用来入侵俄罗斯、中国、伊朗等国的网络系统。调查人员在马丁家中和车内搜出美国政府高度机密文件的复印文本和数字文档，其中数字文档至少有几TB，还包括6份“敏感情报”。美国司法部检察官说，如果在未经授权的情况下泄露这些高度机密文件，美国国家安全将遭受“极为严重”的损害。

引言 —— 2016年信息安全事件

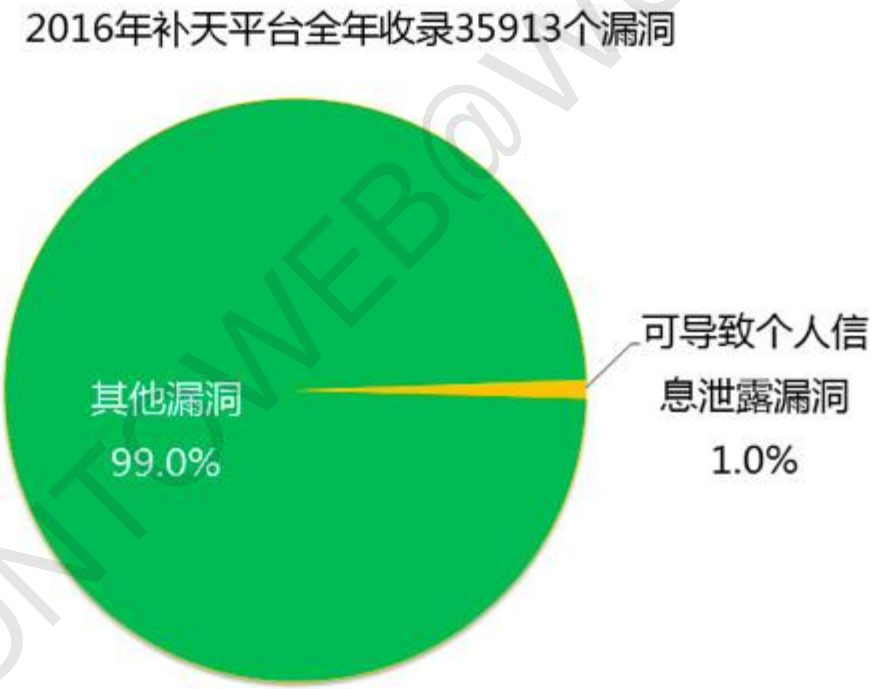
- No.8：全球银行业使用的恐怖嫌疑人数据库被泄露
- No.9：德国核电站检测出恶意程序被迫关闭
- No.10：SWIFT黑客事件爆发 多家银行损失巨款

引言 —— 2016年信息安全事件趋势

- **金融网络安全引发普遍担忧。**孟加拉央行8100万美元失窃巨款，厄瓜多尔Banco del Austro银行约1200万美金被盗，越南先锋银行也被曝出黑客攻击未遂，近一年来黑客利用SWIFT系统漏洞入侵了一家又一家金融机构，俄罗斯也赶上了2016年的末班车，其中央银行遭黑客攻击3100万美元不翼而飞。
- **关键性基础设施成为黑客攻击的新目标。**回顾这一年发生的重大网络安全事件，黑客关注的不仅仅是各种核心数据的窃取，更多的是针对一些关键性基础设施，政府、金融机构、能源行业都成为了黑客攻击新的目标。
- **有政治背景的黑客行动越来越多。**从今年发生的诸多网络安全事件，我们也能看出，有国家支持的政治黑客行动越来越多，未来的网络安全将能影响到一个国家的稳定，网络安全上升到国家高度已成定局

引言 —— 2016年我国个人信息安全现状

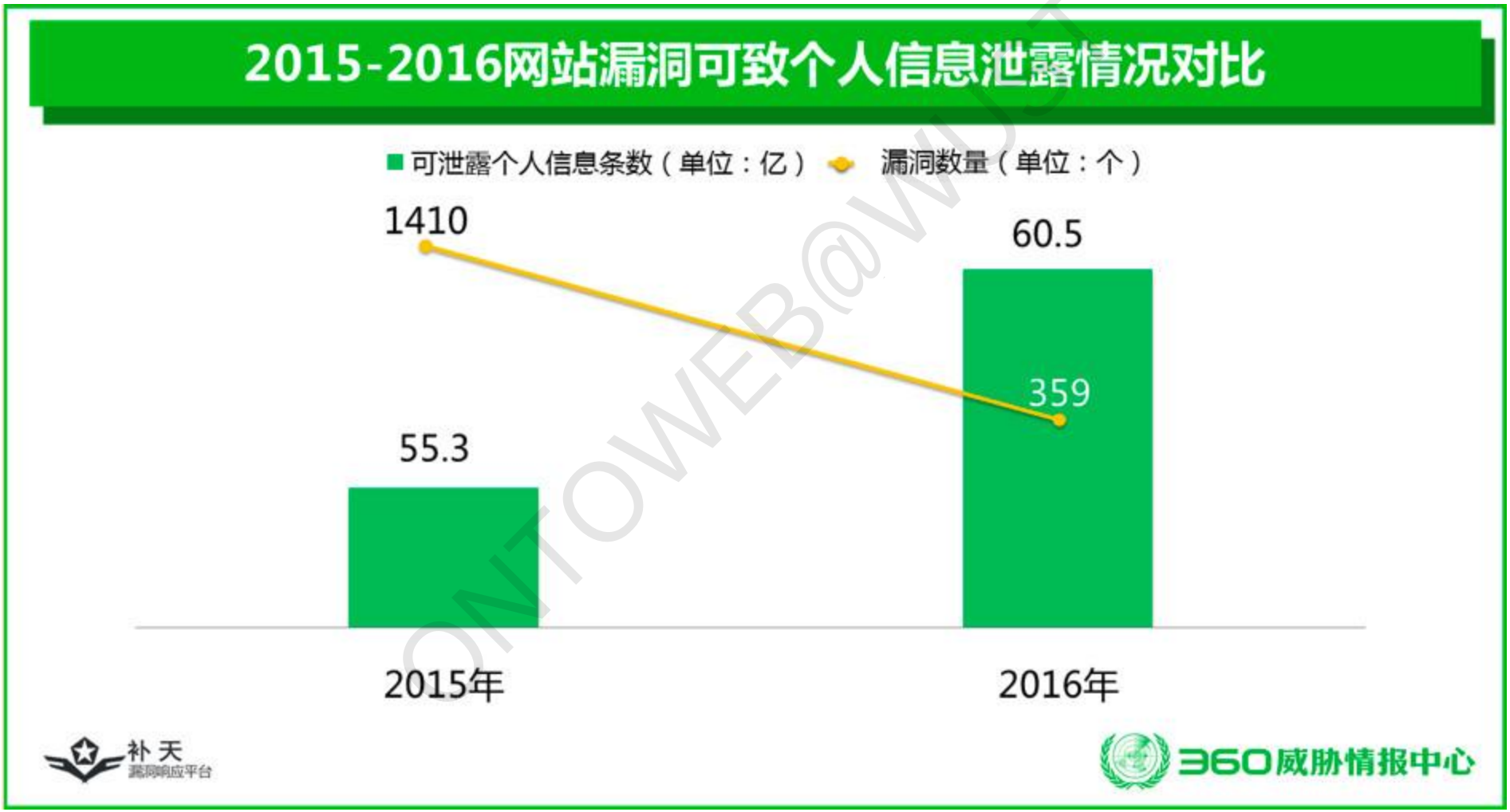
2016年可能导致个人信息泄露网站漏洞数量占比



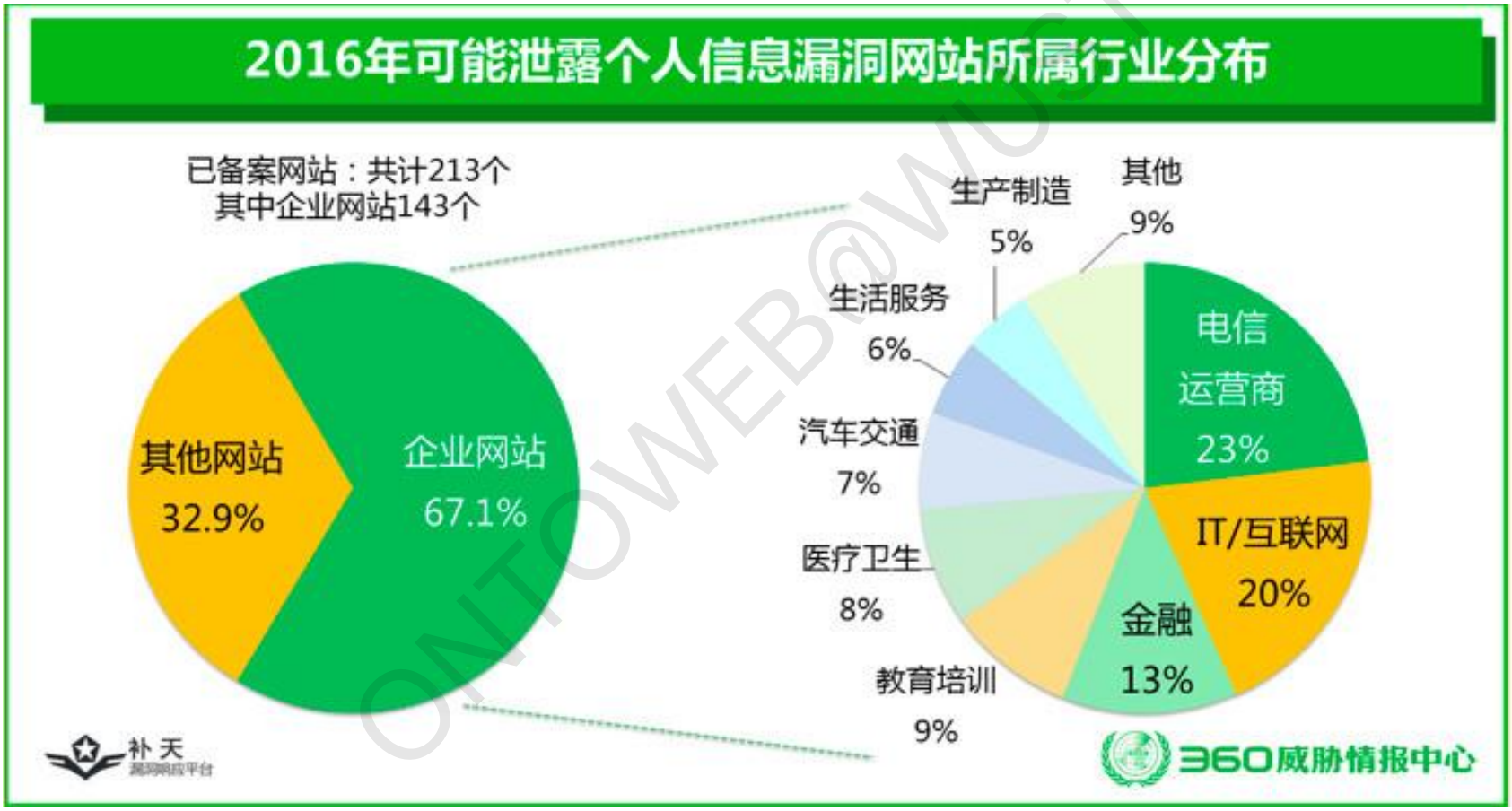
补天 漏洞响应平台

360威胁情报中心

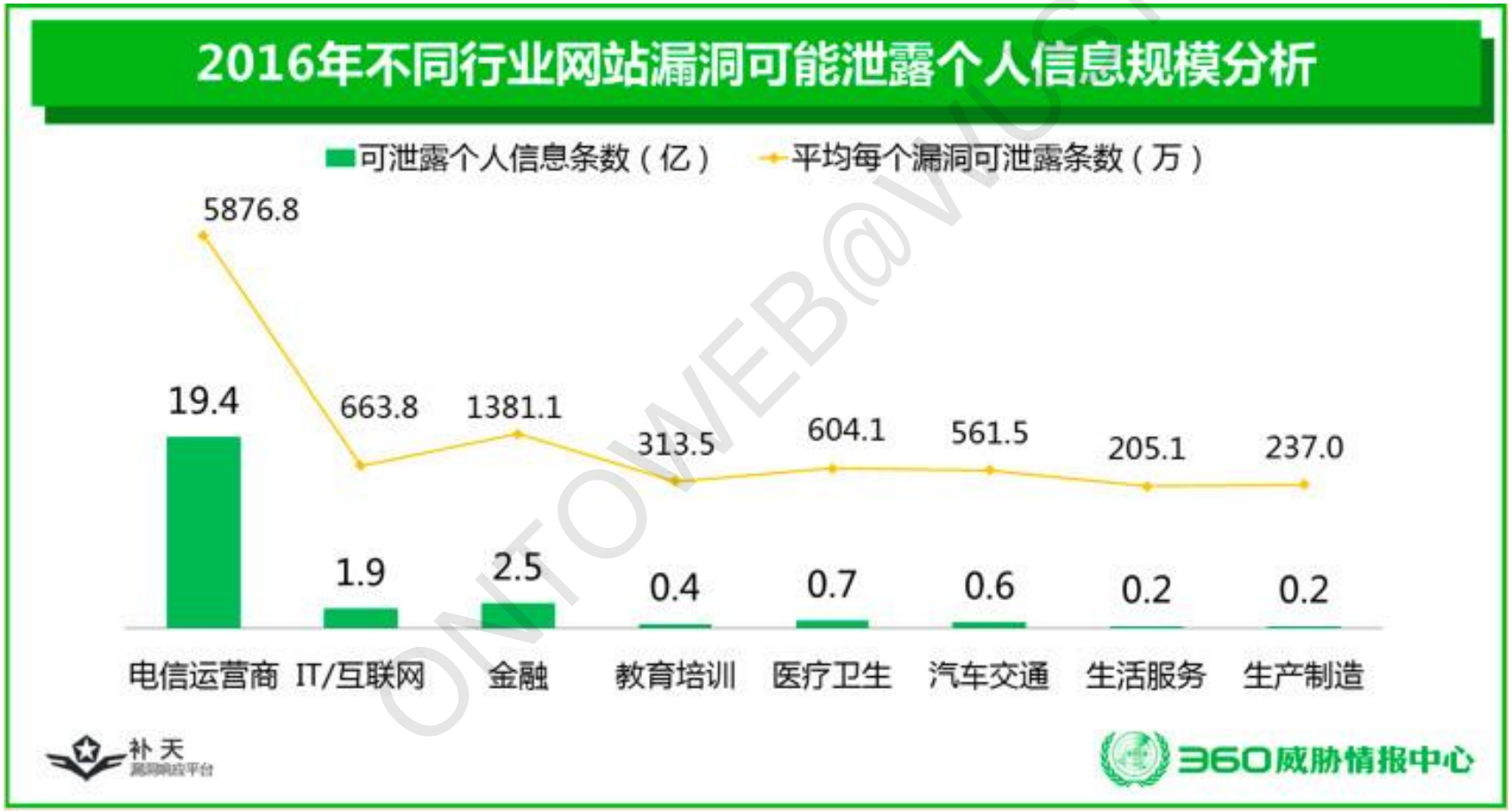
引言 —— 个人信息安全现状



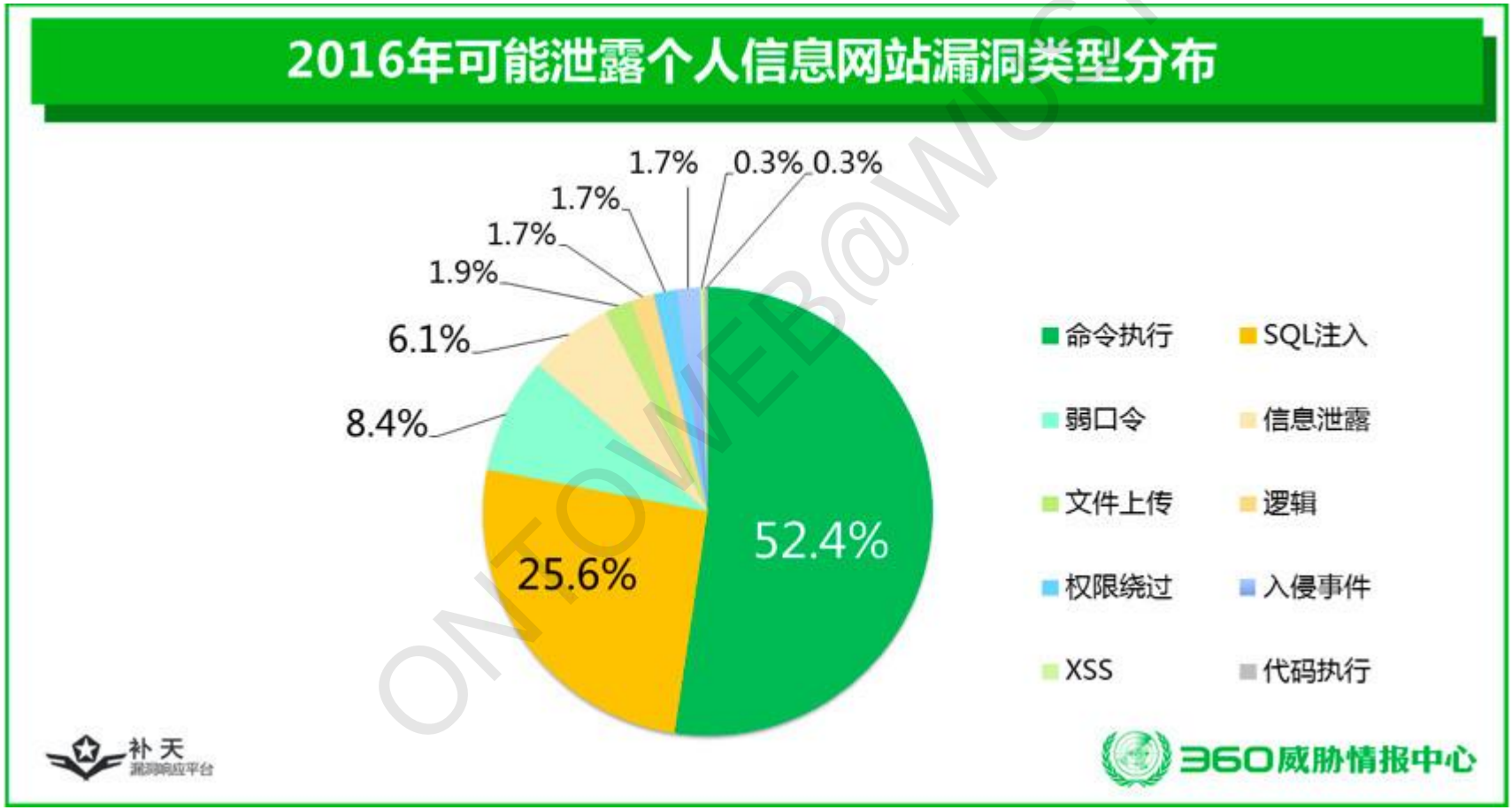
引言 —— 个人信息安全现状



引言 —— 个人信息安全现状



引言 —— 个人信息安全现状



引言 —— 保护你的信息安全

- 养成良好的上网习惯
- 使用正版软件
- 谨慎提供个人信息
- 保持良好的个人密码系统
  - 避免简单密码，和与个人信息有关的密码
  - 密码分级体系
  - 一站一密

网络安全基础

8.1 密码学

密码学（Cryptography）——历史

- 历史上最早的有记录的密码术应用大约是在公元前5世纪。那个时候，古希腊的斯巴达人使用一种叫作scytale的棍子来传递加密信息。

密码学（Cryptography）——历史

- **公元前50年左右，凯撒在军事行动中使用了密码**
  - 明密对照表：
  - 明文：ABCDEFGHIJKLMNOPQRSTUVWXYZ
  - 密文：TUVWXYZABCDEFGHIJKLMNOPQRS
  - 注：广义上的凯撒是位移的。
- **后被16世纪法国亨利三世王朝的布莱瑟·维吉尼亚扩展。**

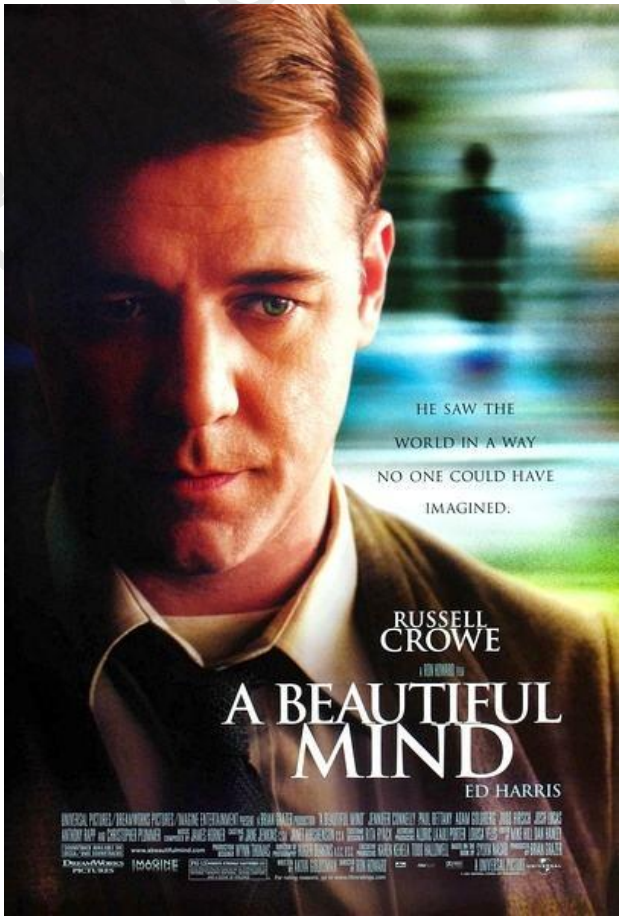
密码学（Cryptography）——历史

- 二战时，在破译德国著名的“恩格玛(Enigma)”密码机密码过程中，电脑之父阿兰·图灵就是在这个时候加入了解码队伍，发明了一套更高明的解码方法。美国人破译了被称为“紫密”的日本“九七式”密码机密码。靠前者，德国的许多重大军事行动对盟军都不成为秘密；靠后者，美军炸死了偷袭珍珠港的元凶日本舰队总司令山本五十六。

密码学（Cryptography）——历史

- 二十世纪五十年代，博弈论之父约翰纳什参与了美国对敌国密码的破译。

- 电影《美丽心灵》



密码学（Cryptography）——历史

第一阶段：古典密码

- 主要依赖算法的保密性。
- 1883年Kerchoffs第一次提出编码原则：加密算法应建立在算法的公开而不影响明文和密钥的安全。

第二阶段：1949~1975

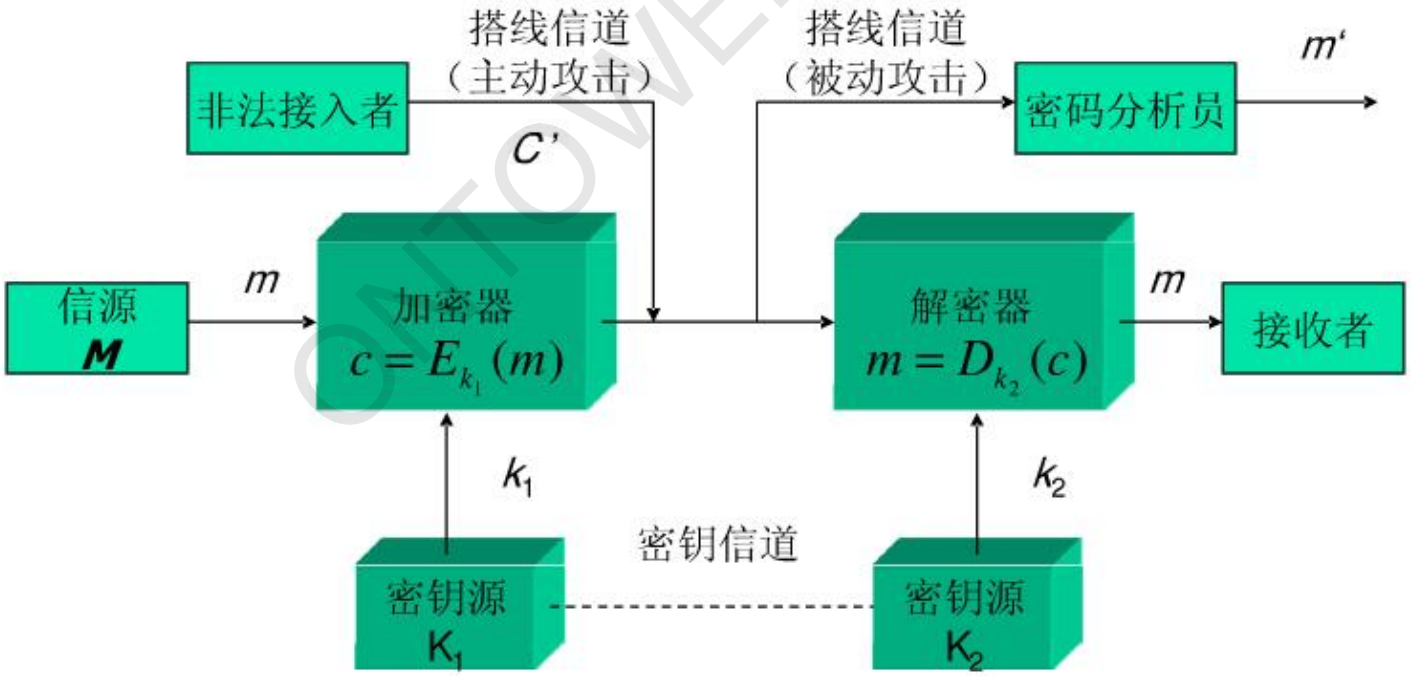
- 计算机使得基于复杂计算的密码成为可能。
- 主要特点：数据的安全基于密钥而不是算法的保密。

第三阶段：1976至今

- 1976年Diffe & Hellman提出不对称密钥
- 1977年提出了RSA（Riverst，Shamir & Adleman），DES。
- 主要特点：公钥密码使得发送端和接收端无密钥传输的保密通信成为可能。

密码学基本概念

- 明文（plaintext）：待加密的消息。
- 密钥（key）：明文以密钥为参数进行某种函数变换。
- 密文（cipher）：函数变换的输出结果。
- 入侵者（intruder）：可能被动监听或者主动插入、回放、篡改消息。



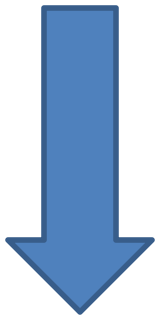
密码学基本概念

- **Kerchoffs原则：所有的算法必须是公开的，只有密钥保密。**
  - 企图让算法保密是不会奏效的。
  - **算法公开会引起讨论和交流，增强算法的安全性。**
- **密码与编码：**
  - 密码（cipher）指逐字逐位对消息进行变换，而不改变消息的语言结构。
  - 编码（code）指用一个词或者符号来代替另一个词，或者使用不同的语言体系来传达消息。如二战时，美军在太平洋战场使用印第安方言对消息进行编码。

密码学基本概念

- 密码学分为密码编码学（cryptography）和密码分析学(cryptoanalysis)。

- 密码分析问题的三个变种：
  - 唯密文攻击：得到了一定量的密文，但是没有明文。
  - 已知明文攻击：得到了一些相匹配的明文和密文。
  - 选择明文攻击：能够加密一些所选择的明文并获得密文。



防御难度递增

置换密码

- 在置换密码中，每个字母或者每组字母被另一个或另一组字母取代，从而将原来的字母掩盖起来。凯撒密码就是一种置换密码。

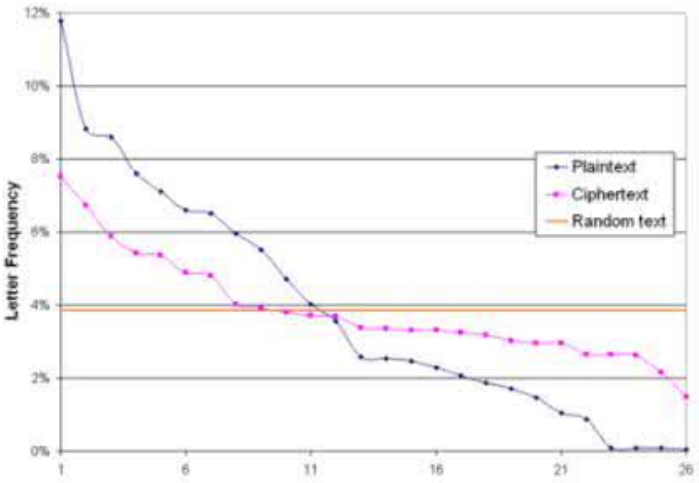
明文字母表：A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

密文字母表：D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

明　　文：HELLO　WORLD

密　　文：KHOOR　ZRUOG

- 密钥有26！个，约$4X10^{26}$个，难以暴力破解。
- 但是易受到字频攻击
- 英文常见字母E,t,o,n,a,i….



转置密码

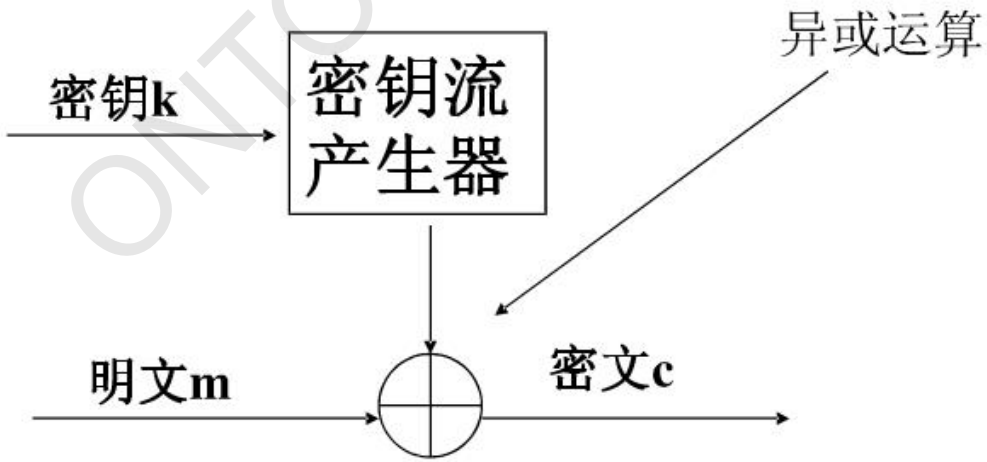
- **在转置密码中，重新对字母进行排序，但并不伪装明文。**
  - 使用某个单词作为密钥（MEGABUCK），对列进行编号，
  - 第一列是密钥字母中最接近‘a’的字母，以此类推。
  - 明文按水平方向书写，密文按列读出。

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

破解方法：
1. 知道/假设为转置密码，
2. 在了解明文的前提下，通过2字组合猜解密钥长度，
3. 两两组合每列分析字频，确定列序。

一次一密

- 在想要构建一个完全不可能被攻破的密码其实相当容易。比如
  - 首先选择一个随机位串作为密钥，
  - 然后将明文变为一个位串（如ASCII码），
  - 逐位计算明文和密钥的异或值作为密文。
  - 每个字符出现的概率相等，组合概率也相等；
  - 密文可能被翻译成任意长度正确且有意义的明文。



一次一密

- **缺点：**
  - 密钥无法记忆，发送方和接收方必须携带密钥副本；
  - 传送的数据量受到密钥数量的限制；
  - 如果丢失字符，或失去同步，后面的数据失效；
  - 一次性密钥的网络传送问题。（量子密码学可能解决）

密码学的两条基本原则

- **密码学原则一：**
  - **消息必须包含一定冗余度。**
  - 冗余是必要的，避免主动攻击者在不理解消息含义的基础上造成麻烦。
  - 冗余同时也会使有效和无效的消息更易区分，导致更容易泄密。

- **密码学原则二：**
  - **需要某种方法对抗重放攻击（如保持消息的新鲜度）。**
  - 在每条消息中加上一个有效时间戳，用于预防主动攻击者不断回放旧的有效信息。

网络安全基础

8.2 对称密钥算法

对称密钥算法

- **定义：**
  - 使用同样的密钥进行加密和解密的算法，也叫私密密钥算法或单密钥算法。
- **特点：**
  - 算法公开、计算量小、加密速度快、加密效率高。
- **例子：**
  - 流密钥算法（一次一密），DES，3-DES，AES(Rijndael)等
- **分类：**
  - 序列密码（流密码）
  - 分组密码（块密码）

分组密码

- 分组密码将明文按照一定的位长分组，明文组和密钥组的全部经过加密运算得到密文组。
- 数据加密标准（Data Encryption Standard, DES）出自IBM，被美国政府正式采纳的数据加密算法（Data Encryption Algorithm, DEA）
- 由中国学者来学嘉和James L. Massey在苏黎世的ETH开发的国家数据加密算法IDEA
- 比利时Joan Daemen和Vincent Rijmen提交，被美国国家标准和技术研究所(NIST)选为美国高级加密标准（AES）的Rijndael。

DES的历史

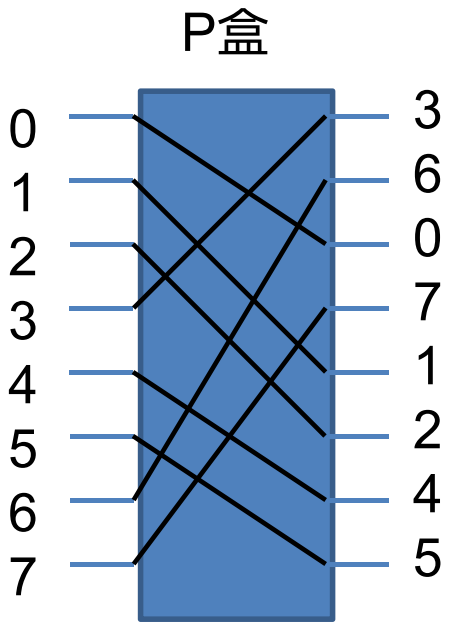
- 1973年，美国国家标准局开始征集联邦加密数据标准的方案
  - Feistel等人研究了一种128位的对称密钥系统，
  - 后IBM改进为56位的密钥系统，并提交NBS。
- 1975年3月17日，NBS公布了IBM公司提供的密码算法，以标准建议的形式在全国范围内征求意见。
- 1977年7月15日，NBS接受了这个建议，数据加密标准DES正式颁布，供商业界和非国防性政府部门使用。

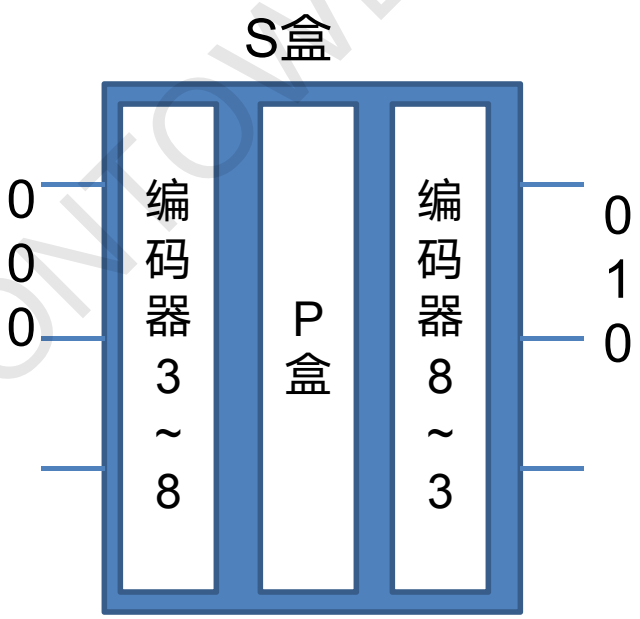
DES的历史

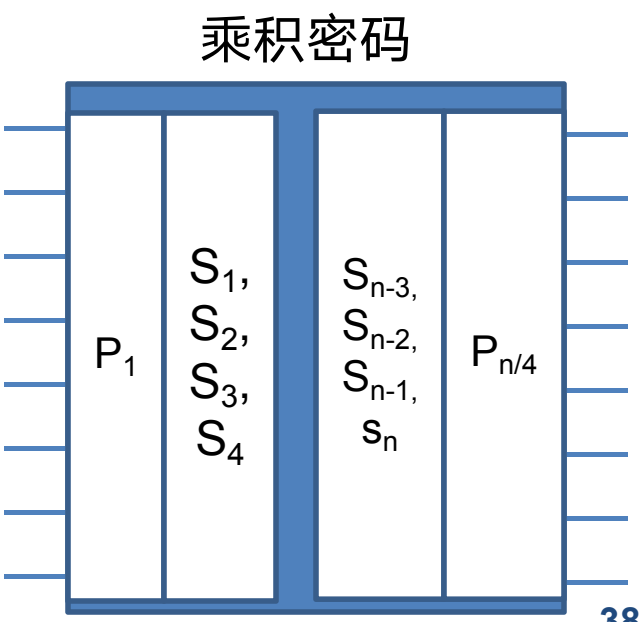
- 1979年，美国银行协会批准使用。
- 1980年，美国国家标准局（ANSI）赞同DES作为私人使用的标准，称之为DEA(ANSI X.392)。
- 1983年，国际化标准组织ISO赞同DES作为国际标准，称之为DEA-1。
- 该标准规定每5年审查一次，计划十年后采用新标准。
- 最后一次评估在1994年1月，决定在1998年12月以后，DES不在作为联邦数据加密标准。
- DES使用**多轮转置和置换**操作进行加密。

乘积密码

- P盒： 执行**转置**操作（Permutation），改变数据位的顺序。
- S盒： （利用P盒）执行**置换**操作（Substitution），使用其他数据替代数据位数据。
- 乘积密码：使用**多次转置和置换**操作，构造复杂转换函数。
- 乘积密码的高复杂度是DES的基本原理。







DES的描述

- DES利用56比特长度的密钥K（还有8位的同步位密钥）来加密64位的明文，得到长度64位的密文。

初始转置和初始逆转置

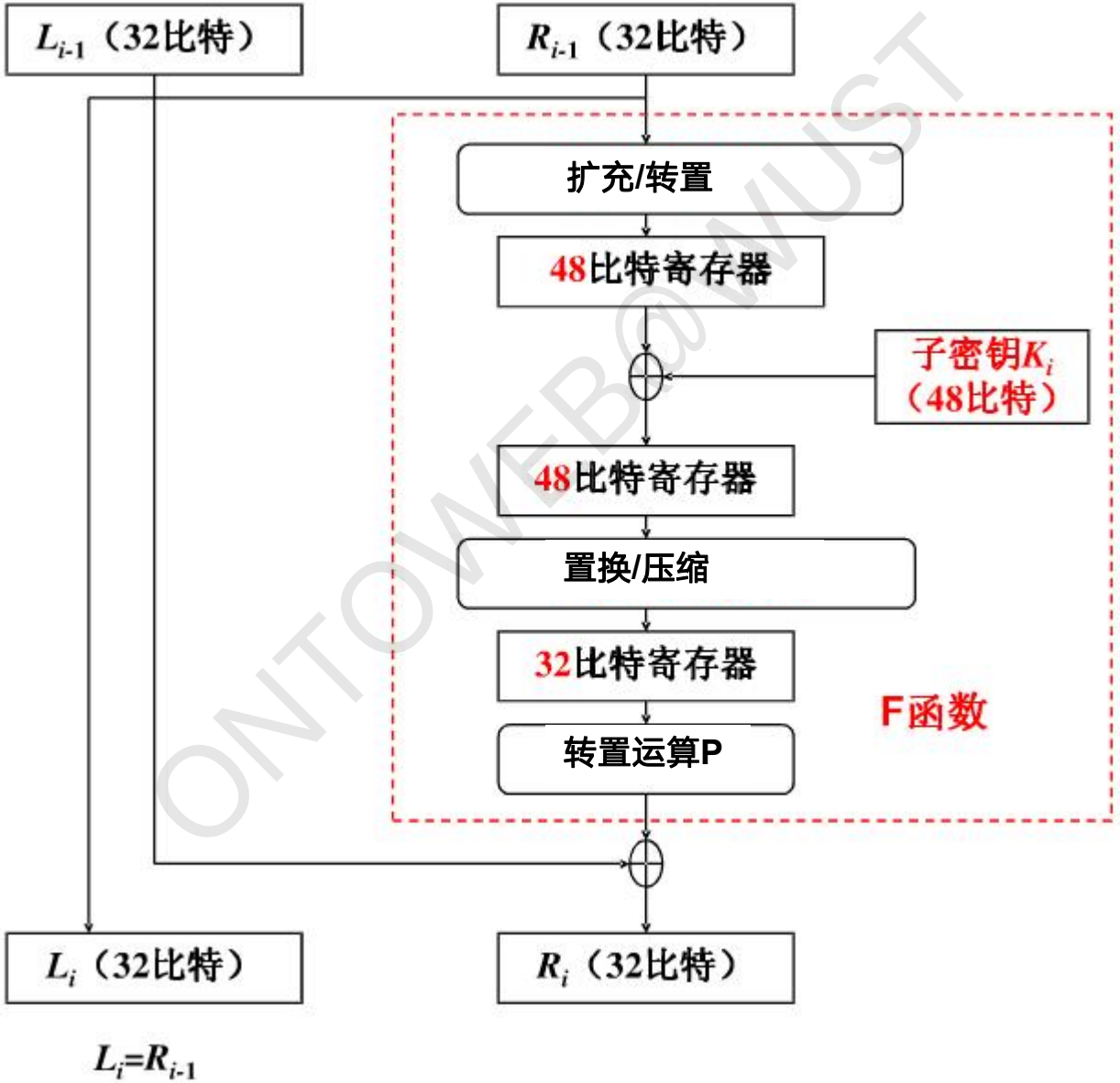
初始置换 IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

初始逆置换 IP^{-1}

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

DES的每轮迭代



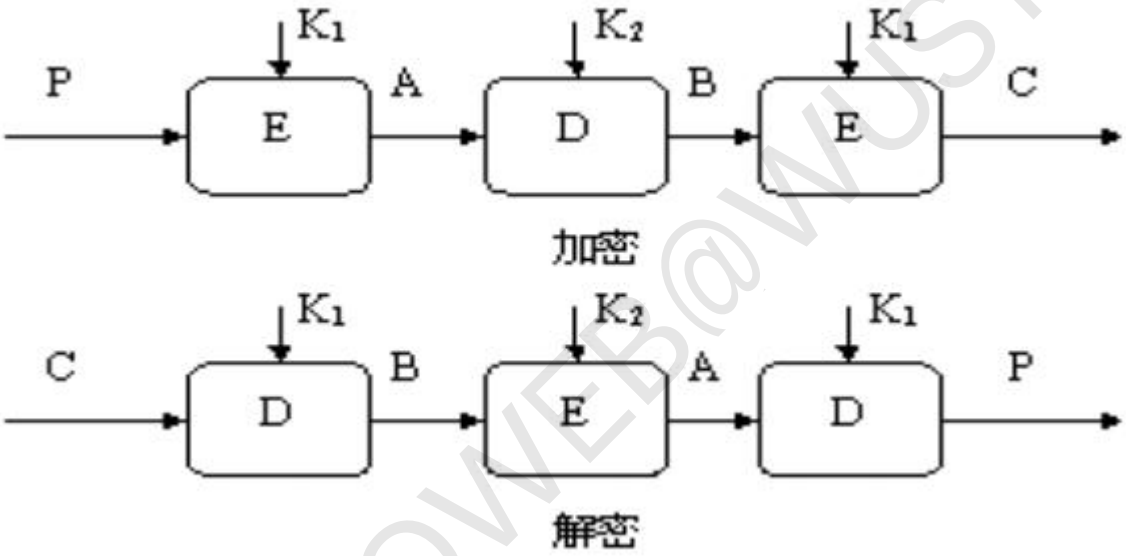
DES的争议和破解

- 有批评认为IBM将128位密钥缩短为64（56），并保密设计过程，造成了DES的安全性弱。
- 甚至有人认为NSA（职能之一为破解密码）约谈IBM“讨论”DES是为了在DES中留下后门，确保只有NSA能破解DES。
- 1997年，斯坦福的两位研究员Diffie和Helman设计了能破解DES的机器。给定一小段明文和匹配的密文，这台机器能在一天内穷举出密钥（共2^56个密钥）。

三重DES

- 1979年初，IBM意识到DES的密钥长度太短，于是设计了一种方法，利用三重加密来有效增加密钥的长度。
- 三重DES的四种模型：
- DES-EEE3：三个不同的密钥，三次加密；
- DES-EDE3：三个不同的密钥，两次加密一次解密；
- DES-EEE2：K1=K3;
- DES-EDE2：K1=K3

双密钥的三重DES



- 使用2个密钥而不是三个，主要因为2个共112位密钥已经足够了，第三个密钥带来额外的密钥管理开销。
- 使用EDE而不是EEE主要为了和使用单DES的计算机兼容：设置K1=K2即可。

高级加密标准AES

- 随着DES和3-DES慢慢走向尽头，美国标准和技术委员会（NIST）开始着手建立新的数据加密标准。
- NIST在1997年发起一场密码学比赛，希望产生一个高级加密标准（AES），规则如下：
  - 1，它必须是一个对称的块密码算法。
  - 2，必须公开所有设计。
  - 3，必须支持128,192,256位密钥长度。
  - 4，必须在软件和硬件上能够方便实现。
  - 5，算法必须公有，或无偿授权给所有人使用。
- NIST在2000年10月宣布Rijndael（音Rhine-Doll）算法胜出。、
- Rijndael密钥空间为2^128，暴力穷举是（几乎）不可能的。

分组密码的使用模式

模式	描述	典型应用
电子密码本ECB	用相同的密钥分别对明文分组加密	单个数据的安全传输
密码分组链接CBC	加密算法的输入是上一个密文分组和下一个明文分组的异或	普通目的的面向分组的传输
密码反馈CFB	一次处理J位，上一个分组密文作为产生一个伪随机数输出的加密算法的输入，该输出与明文分组异或，作为下一个分组的输入	普通目的的面向分组的传输认证
输出反馈OFB	与CFB相同，只是加密算法的输入是上一次DES的输出	噪声信道上数据流的传输（如卫星传输）
计数器模式CTR）	每个明文分组是加密的计数器的异或，对每个后续的分组，计数器是累加的。	普通目的的面向分组的传输用于高速需求

分组密码的典型攻击方式

- **强力攻击：最可靠的方式**
  - 穷尽密钥搜索；
  - 字典攻击；
  - 查表攻击；
  - 混合攻击。
- **差分密码攻击：最有效的方式**
  - 通过明文对的差值对密文对差值的影响来回复某些密钥位。
- **线性密码攻击：**
  - 本质上是已知明文攻击，通过寻找一个给定密码算法的有效的线性近似表达式来破译密码。
- **功率消耗攻击，时间分析攻击**

网络安全基础

8.3 公开密钥算法

为什么设计公开密钥算法

- **密钥管理问题：**
  - 每对用户需要使用一个密钥，N个用户需要C(N,2)个密钥。当用户数量增大，密钥量迅速变多。
  - 用户的密钥由密钥分发中心（KDC）管理，KDC必须被信任，但有可能被攻破。
- **对称密钥难以实现抗抵赖的算法（认证）**

公开密钥算法的起源

- 公钥密钥又称双钥密码或非对称密码，1976年由Diffe和Helman在其划时代的文献“密码学新方案”中提出。他们对加密算法E和解密算法D提出了3个要求：
  - D(E(P)) = P，且E(D(P)) = P；
  - 从E推出D极其困难；
  - 选择明文攻击不可能破解E.
- 1978年RSA算法被提出。

公开密钥算法的特性

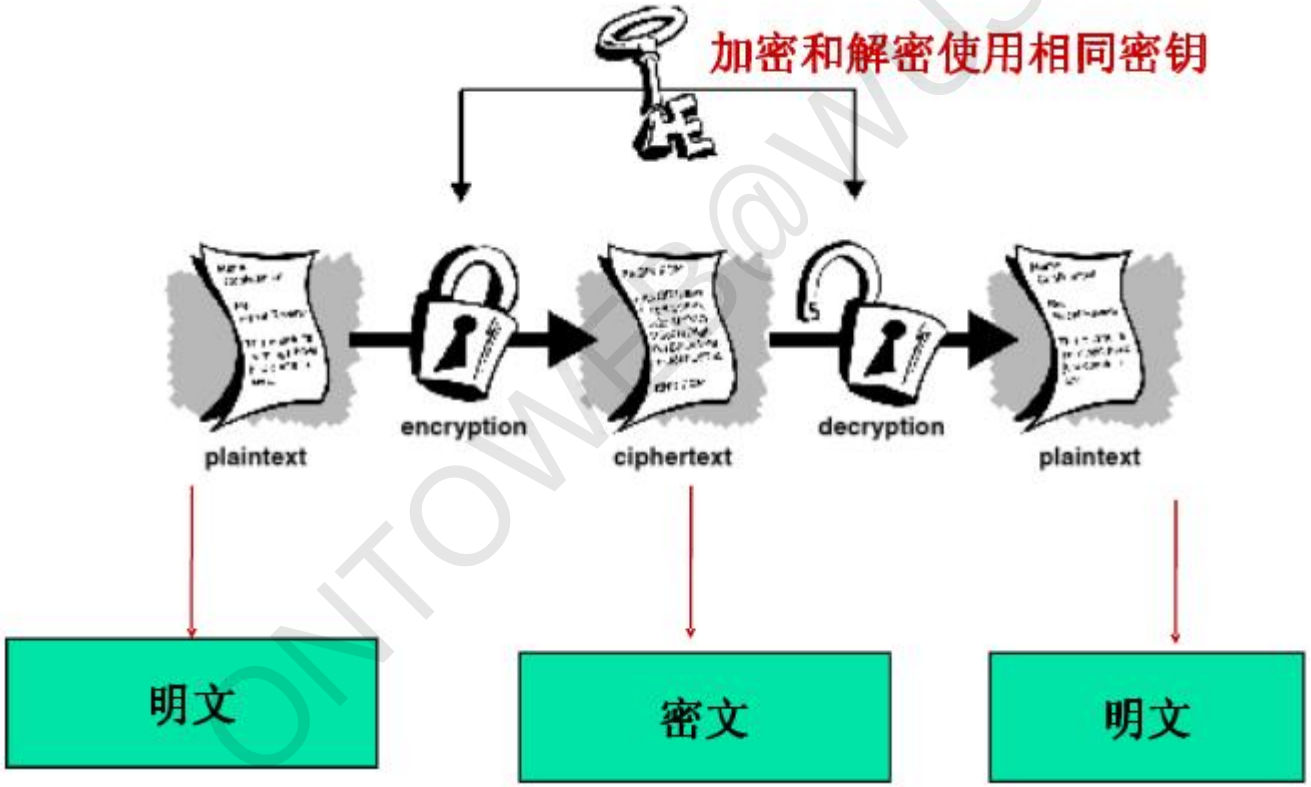
- 加密与解密由不同密钥（K,B）完成
  - 加密： P->C: $C = E_K(P)$
  - 解密： C->P: $P = D_B(C)$

    $= D_B(E_K(P))$

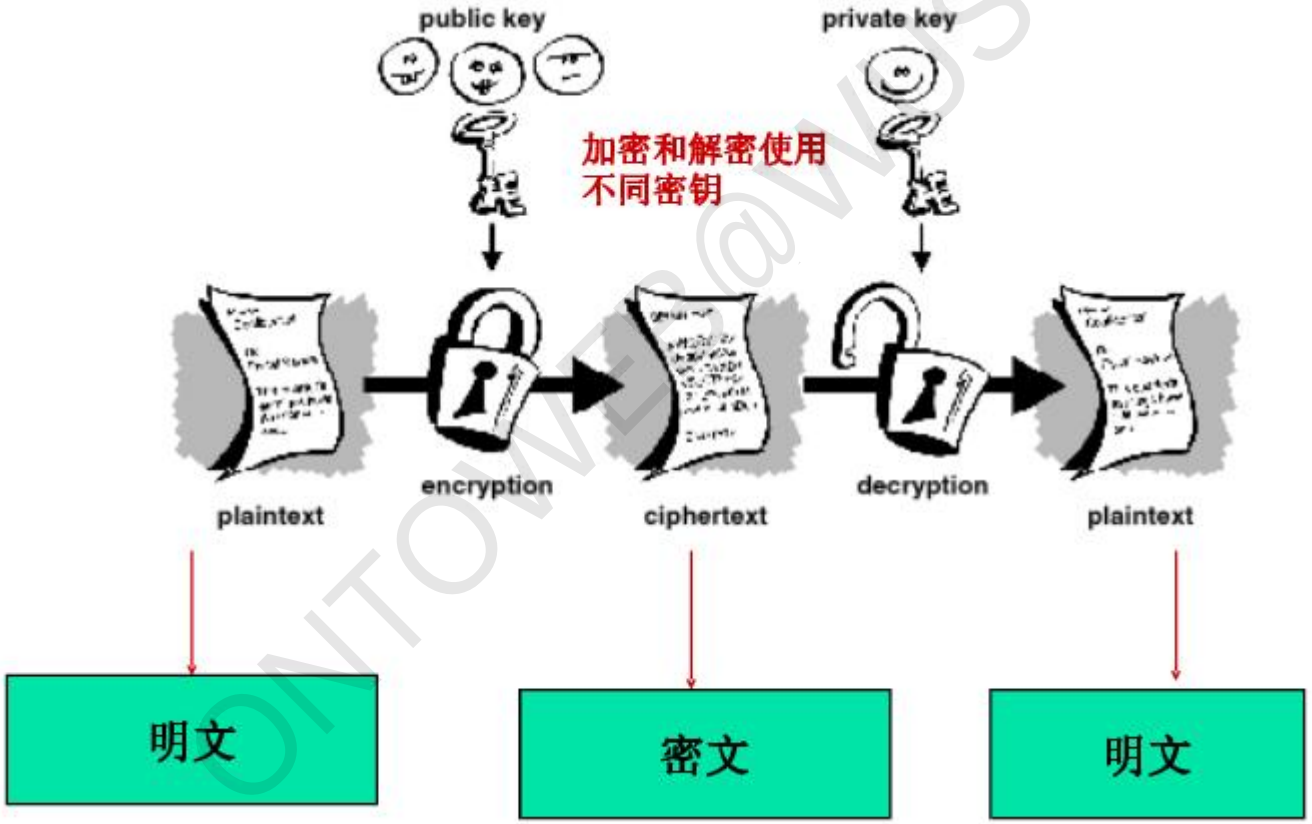
- 知道加密算法，从加密密钥不能计算出解密密钥。
- 两个密钥中的任意一个都可以用为加密，另一个作为解密（非必须）。

$$P=D_B(E_K(P))=E_K(D_B(P))$$

传统加密过程

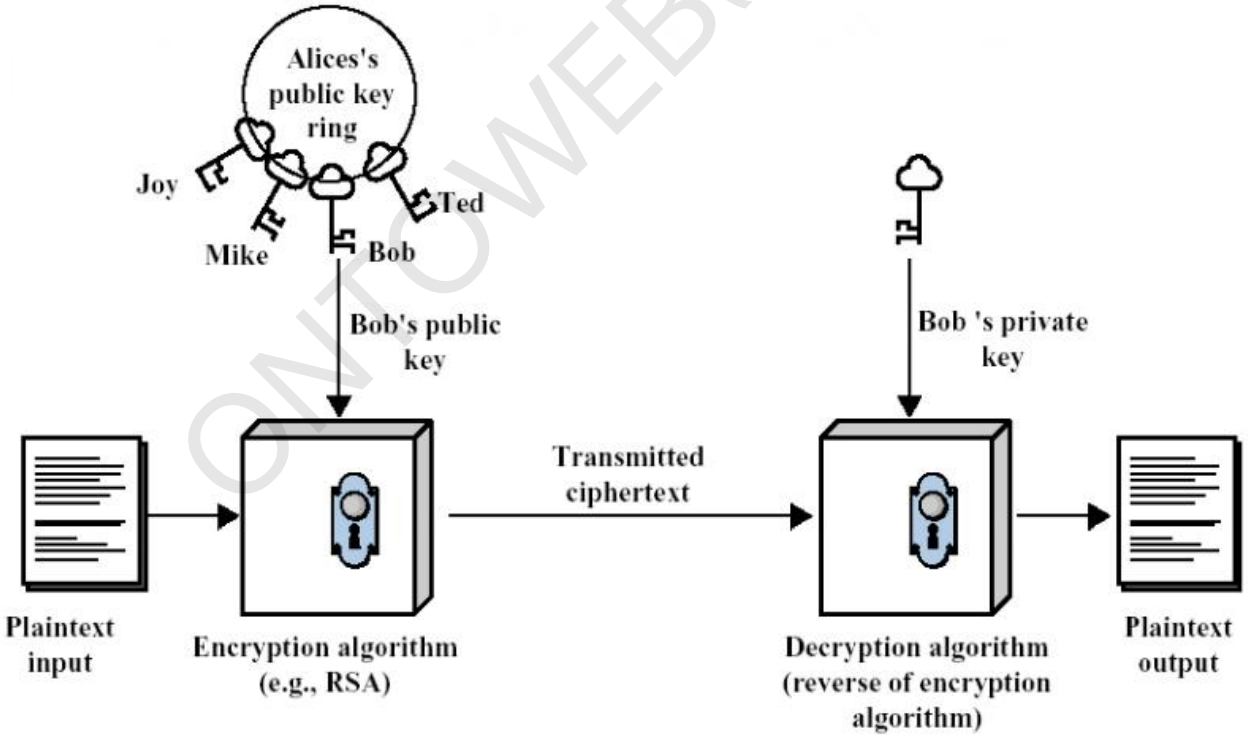


公钥加密过程



使用公钥实现保密

- **用户拥有密钥对（k，k’）公钥k公开，私钥k’保留**
  - Alice -> Bob：C= $E_{kb}(P)$
  - Bob： $D_{kb'}(C)=D_{kb'}(E_{kb}(P)) = P$



公钥算法的要求

- 产生一堆密钥是计算可行的。
- 已知公钥和明文，产生密文是计算可行的。
- 接收方利用私钥来解密密文是计算可行的。
- 对于攻击者，利用公钥来推断私钥是计算不可行的。
- 已知公钥和密文，恢复明文是计算不可行的。
- 加密和解密的顺序可以交换。（可选）

单向陷门函数

- 单向陷门函数（单陷门函数）f满足下列条件：

- （1）给定x，容易计算 $y = f(x)$
- （2）给定y，计算x使得 $x = f^{-1}(y)$是不可行的。
- （3）存在k（陷门），已知k时，对任意给定的y，如果x存在，则容易计算 $x = f^{-1}(y)$

RSA概述

- **安全性建立在大数因式分解的困难性上：**
  - 已知2个素数p, q；计算 n=pq是容易的；
  - 但是已知n，求pq是困难的（NP完全问题）。

- **RSA的缺点主要是密钥太长（一般是1024位），速度较慢。**

RSA算法概要

1. Bob选择保密的素数p和q，并计算n=pq；
2. Bob通过gcd(e, (p-1)(q-1))=1来选择e；
3. Bob通过de≡1(mod(p-1)(q-1))来计算d；
4. Bob将n和e设为公开的，p、q、d设为秘密的；
5. Alice将m加密为$c \equiv m^e \pmod{n}$，并将c发送给Bob；
6. Bob通过计算$m \equiv c^d \pmod{n}$解密。

RSA算法例子

1. 选择两个素数: $p=17$ & $q=11$
2. 计算 $n = pq = 17 \times 11 = 187$
3. 计算 $\phi(n)=(p-1)(q-1)$

   $=16 \times 10=160$
4. 选择 e ; $\gcd(e,160)=1$; 其中 $e=7$

RSA算法例子

5. 计算d：$de=1 \bmod 160$ 且 $d < 160$，则 d=23 （因为23×7=161=10×160+1）
6. 公布公钥$K_U=\{7,187\}$
7. 保存私钥$K_R=\{23,17,11\}$

RSA算法例子

- 如果待加密的消息 M = 88 (注意：88<187)
- 加密：$C = 88^7 \bmod 187 = 11$
- 解密:$M = 11^{23} \bmod 187 = 88$

RSA加密与解密函数互为反函数，证明略

可用于公钥算法的数学难题

- 大整数的因式分解问题（RSA基础原理）。
- 背包问题（Merkle & Hellman, 1978）。
- 有限域的乘法群上的离散对数问题。（El Gamal，1985）
- 椭圆曲线上的离散对数问题。（Menezes & Vanstone，1993）。

背包问题

- 已知一个容量为B的背包，以及重量为a1，a2，… an的n个物品。若从这N个物品中选出若干个正好可以装满这个背包，现在问，有哪些种可能的物品列表？

- 基于背包问题的公钥算法发明者 Ralph Merkle确信这个算法不会被攻克，悬赏了100美元给破解者，Adi Shamir（RSA中的S）很快破解了算法领取奖金，Merkle没有气馁，改进了算法并悬赏1000美元，又被Ronald Riverest（RSA中的R）破解。后来Merkle并没有为后续版本悬赏10000美元（RSA中的Adleman的不幸）

网络安全基础

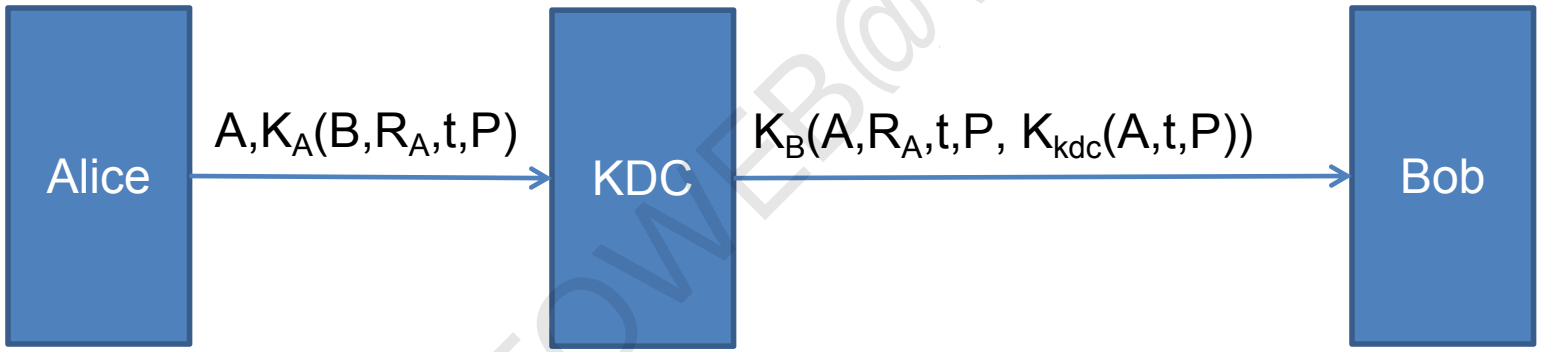
8.4 数字签名

数字签名的要求和特性

- 在传统行业中，手写签名被广泛使用，并用以确认文档的真实性。（影印无效）。在计算机上实现签名的功能比较困难，有如下的要求：
  - 接收方可以验证发送方的身份，
  - 发送方以后不能否认消息的内容，
  - 接收方不可能自己编造该信息。

对称密钥系统中的认证

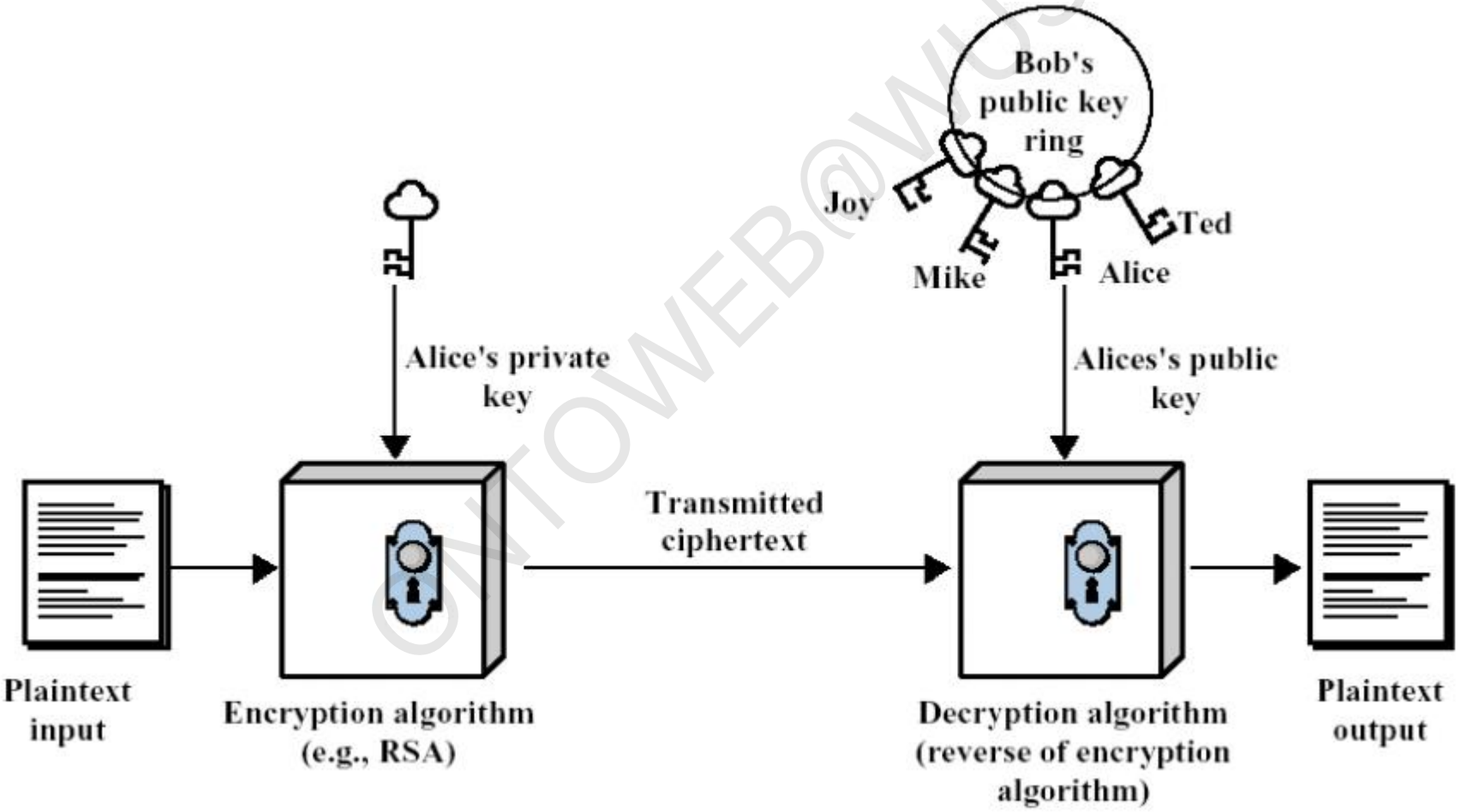
- Alice和Bob把自己的密钥交给KDC，然后消息经由KDC转发，这样KDC可以对A和B的消息进行认证。



- 人人都需要信任KDC，KDC可以解读所有签名的信息，醉可能运行KDC的是政府、银行、会计事务所、律师事务所等，可惜人们往往并不完全信任他们。

公钥系统中的认证

- Alice用自己的私钥进行加密，Bob用Alice的公钥解密



公钥系统中的保密与认证

- 利用E(D(P)) = P的属性
- Alice -> Bob: $C=E_B(D_A'(P))$
- Bob: $E_A(D_B'(C))$

  $=E_A(D_B'(E_B(D_A'(P))))$

  $=P$

消息摘要

- **明文签名的缺点：**
  - 将认证和加密耦合，往往很多地方只需要认证不需要加密；
  - 签名算法太慢。
- **消息摘要（Message Digest, MD）以单向散列函数作为基础，将任意长度的明文变为一个固定长度的位串，这个散列函数满足：**
  - 给定P，很容易计算MD(P)；
  - 给定MD(P)不容易恢复P；
  - 给定P，没人能找到P’使得MD（P’）=MD(P)；
  - P即使改变1位，也会导致完全不同的输出。

消息摘要

- **目前有两种主要的消息摘要函数：**
  - MD5（Riverest, 1992），是Riverest设计的第5个摘要算法，已经存在了20多年，已经被部分破解，但是内在的一些屏障仍未沦陷，目前仍在使用。处理512位的块，提供128位的摘要。
  - SHA-1，由NSA开发，收到NIST赞赏，处理512位的明文块，得到160位的摘要。SHA有些新版本正在开发中，提供256,384和512位的散列值。

网络安全基础

8.5 通信与WEB安全

IPSec

- IETF一直以来都明白Internet存在的安全性问题，对于在Internet的哪里加入安全性，曾经存在一些争议。

- 大多数安全专家认为，为了做到真正的安全，必须提供端到端的安全协议（也就是在应用层上），包括数据的加密以及完整性保护。但是这样需要改变所有的应用系统，因此次好的选择是在传输层上实现安全(SSL/HTTPS)。

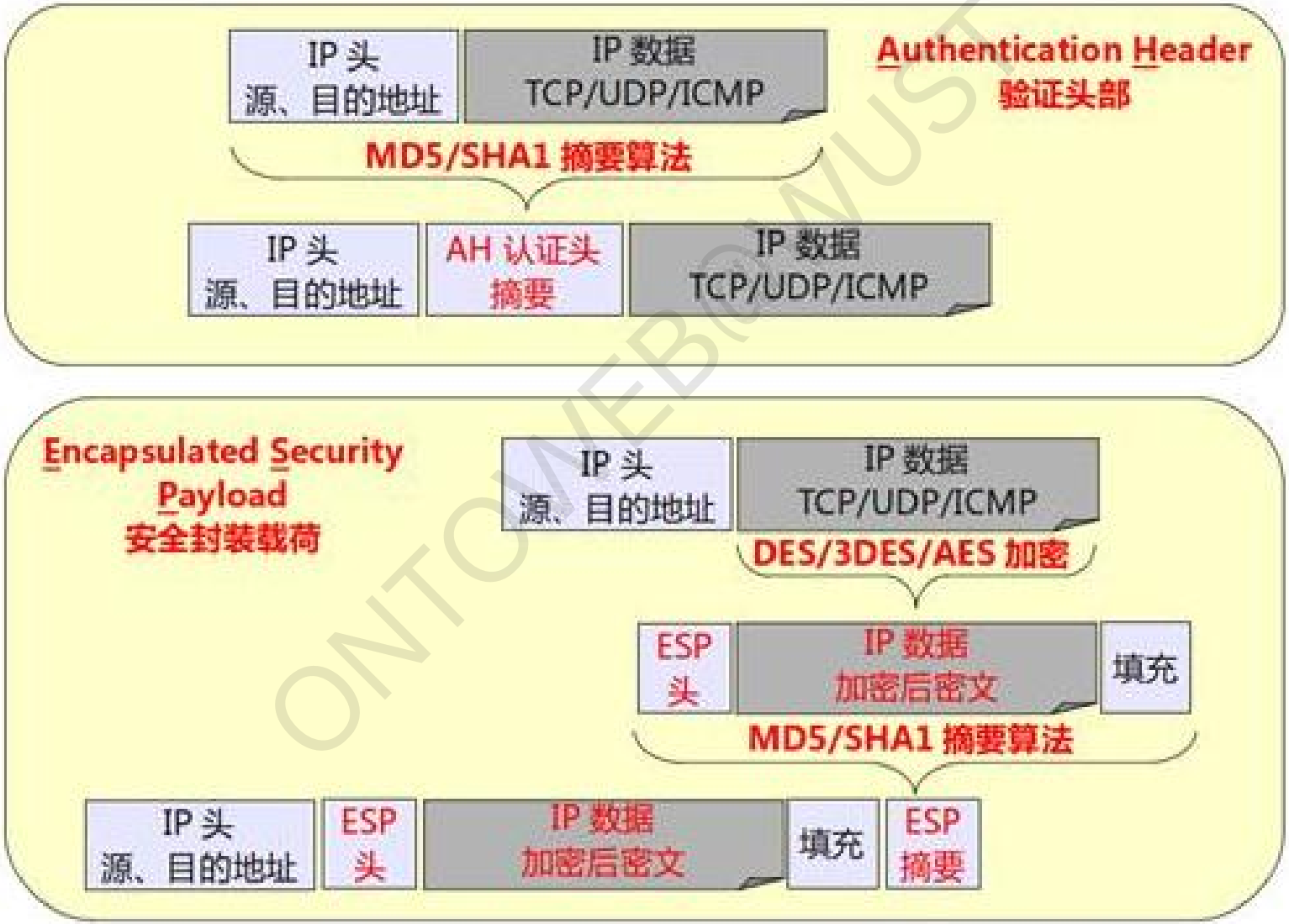
- 相反的观点认为，用户并不理解安全性，也无法正确使用安全性，且没有人愿意以任何方式修改已有的程序，所以网络层应该提供认证或者加密分组。

- IPSec是第二种观点取胜的产物。

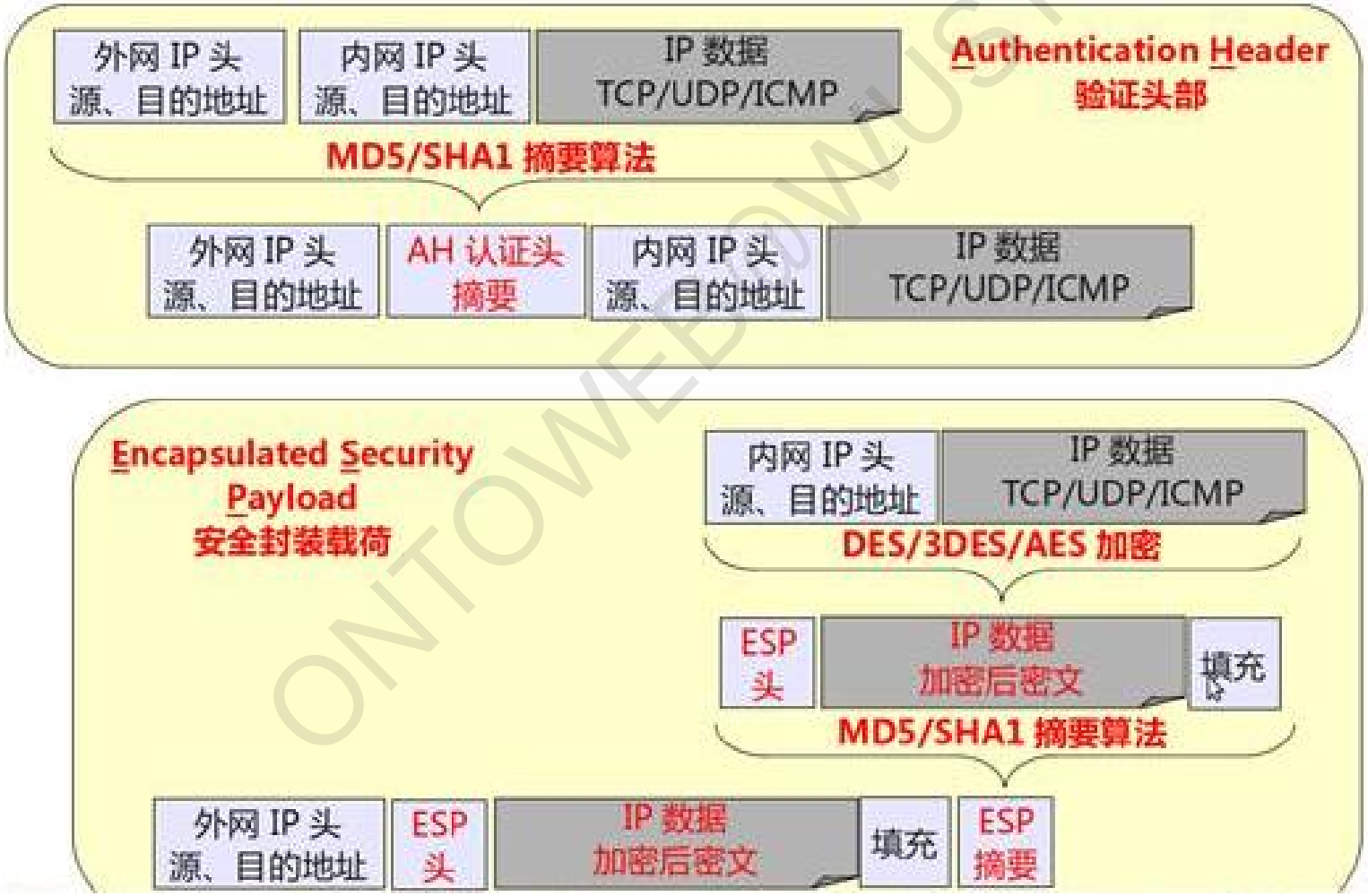
IPSec

- **IPSec在IP数据包种引入了两种新的头信息：认证头（AH）和封装安全载荷头（ESP）**
  - AH只提供认证，不提供加密，
  - ESP提供认证和加密。
  - ESP功能更多，效率实际也更高，AH以后可能会慢慢淘汰。
- **IPSec有两种工作模式：传输模式和隧道模式**
  - 传输模式不改变原来的IP头，只在IP头后面增加一个头部信息，常用于端到端的传输。
  - 隧道模式创建一个新的IP头，可以用于各种场景，但对于PC到PC的传输额外开销太大，一般隧道模式用于站到站的传输，安全封装信息止于一台网关安全机器，如某公司的防火墙，而LAN中的机器不必知晓IPSec。

IPSec——传输模式



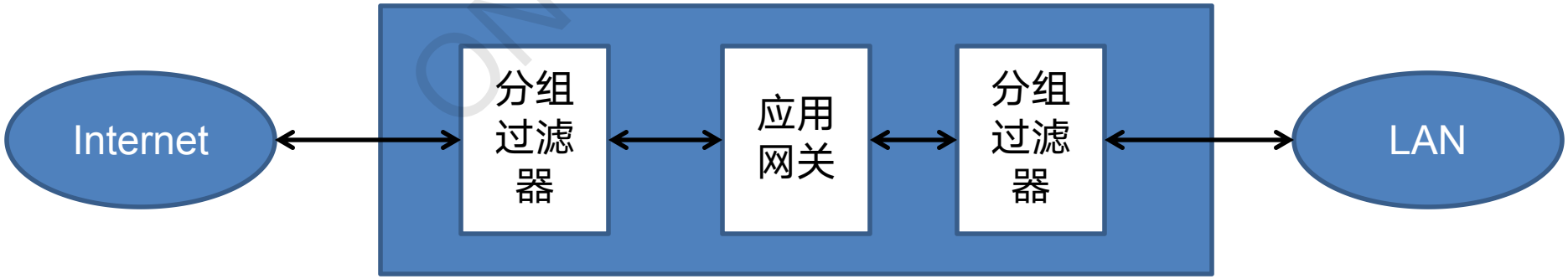
IPSec——隧道模式



防火墙

- IPSEC可以有效的阻止伪造信息，并提供信息的安全传输，但是并不能阻止有害信息的传输。因此需要防火墙。

- 防火墙通常有2个分组过滤器和一个应用网关组成。
  - 分组过滤器是配置了额外功能的路由器，可以用来阻塞某些有害站点和端口。
  - 应用网关运行在应用层上，如配置一个邮件网关来检查头部信息，消息长度甚至消息内容来决定转发或者丢弃邮件。



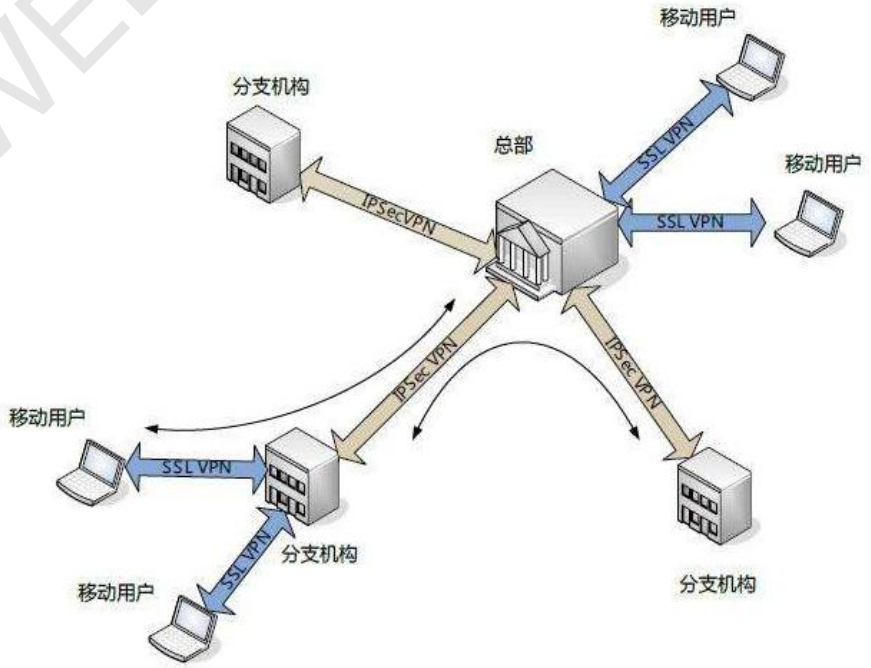
拒绝服务攻击（Denial of Service）

- **攻击者的目标不是窃取数据或者进行欺诈，而是单纯的瘫痪站点。**
  - 向目标机器发送大量的TCP SYN请求，Web站点会发送一个Syn+ACK回应，如果攻击者不再相应，这个表项会被占用一定时间，直到超时。过多的请求会占用所有表项，而使得Web站点无法正常工作。
  - 一般来说这种请求的原地址被伪造，从而避免追踪。
  - 更糟糕的是，攻击者可能入侵了全世界的几百台甚至上千台计算机，命令所有机器同时发起攻击，这样的攻击就是DDoS.
  - 即使服务器能快速识别伪造的请求，也必须花一定时间来进行处理，如果请求数目足够多，仍然可以瘫痪服务器。

虚拟私有网络

- 过去（在公用数据网之前）公司往往从电话公司租用线路，将分布的办公场所连接起来，建立私有网络。
- 私有网络非常安全，因为它与外界隔绝，但是开销太大，因此产生了基于因特网的虚拟私有网络（Virtual Private Networks）

  - 每个场所配备一个防火墙，并在每两个防火墙之间建立IPSec隧道。
  - 防火墙，基于ESP的IPSec和VPN通常结合在一起，被广泛应用。



WIFI的安全问题

- 2001年9月7日，IEEE对WEP(Wired Equivalent Privacy)加密标准被完全攻破做出了响应，并发表了一个简短的声明：
  - 我们告诉你，WEP的安全性并不比以太网更好；
  - 一个更大的威胁是忘记启用安全功能；
  - 请尝试使用其他种类的安全设施（如传输层安全性）；
  - 下一版本的802.11i将提供更好的安全性；
  - 将来将强制使用802.11i；
  - 在802.11i来到之前，我们会尽力寻求解决办法。

WEB安全

- **WEB安全可以分为三个部分：**
  - 安全的命名资源和对象：
    - DNS欺诈，和安全的DNSsec
  - 建立安全的连接：
    - 1995年网景公司（NETSCAPE浏览器公司）在应用层和传输层之间引入了新的安全套接字层（SSL）用以建立安全的连接（HTTPS），功能包括：C/S参数协商，双向认证，保密通信，数据完整性保护。
  - 安全的可执行代码：
    - JAVA APPLET：在浏览器内建的解释器中执行，并对命令检查；
    - ActiveX：控件都需要代码签名；
    - JavaScript：没有任何正式、标准的安全模型，存在较多漏洞；
    - 病毒和木马：感染可执行程序，并自我复制传播，病毒通常恶意破坏数据，而木马则偷偷窃取信息。微内核系统可能有助于抑制病毒和木马。