



智能环境下数据安全与应用创新模式

北京大学 信息工程学院

朱跃生

2022年12月

北京大学



网络安全-国家一级学科

➤ 五大空间

领土

领空

领海

太空

网络空间



信息安全基本知识

传统保护信息安全手段（电脑出现前）

□ 物理手段 (physical)

保险柜：防止被盗窃、毁坏、非法阅读或篡改

图章或签名：表明档的真实性和有效性

铅封：防止文件在传送中被非法阅读或篡改

□ 行政手段 (administrative) (政策)

文件管理制度：

机密等级

行政级别

□ 密码学手段：

密文

安全隐患

自身缺陷 + 开放性 + 骇客攻击

互联网的特点：

开放性、交互性、分布性、互连性

发明时，根本没有考虑安全问题与用户的诚信

业务基于公开协议

远端存取

连接基于彼此信任

骇客 (Hacker) 攻击

“非法入侵者”

目的:

- 基于兴趣
- 基于利益
- 基于捣乱

信息安全的挑战

Copy: 复制后的文件跟原始档没有差别

Modify: 对原始档的修改可以不留下痕迹

Signature: 无法在文件上直接签名或盖章

Transmit: 在传送中可被非法阅读或篡改

Storage: 在保管中可被盗窃、毁坏、非法阅读或篡改

Method: 信息安全无法完全依靠物理手段和行政管理

安全服务 (Security Services)

- **保密** Confidentiality (privacy)
- **鉴别** Authentication (who created or sent the data)
- **完整** Integrity (has not been altered)
- **不可抵赖** Non-repudiation (the order is final)
- **存取/接入控制** Access control (prevent misuse of resources)
 - **可用** Availability (permanence, non-erasure)
 - prevent
 - Virus that deletes files
 - Denial of Service Attacks

为什么需要密码算法

- 信息存储:存放在**公开**的地方
- 信息交换:使用**非隐秘**介质
- 信息传输:通过**不秘密**频道

密码学

- 密码学：

研究与信息安全相关的方面如机密性、完整性、实体鉴别、抗否认等的数学理论。

由**密码编码学**和**密码分析学**构成。

- 密码**编码学**的基本目标：

– 机密性、数据完整性、鉴别、抗否认

- 基本的密码工具：

加密、散列函数、数字签名

密码分析学 Cryptanalysis

□ 方法

cryptanalytic attack **密码分析攻击**

系统分析法（统计分析法）：利用明文的统计规律

确定性分析法

brute-force attack **强力法 或称 穷举攻击**

对截获的密文依次用各种可能的密钥破译。

对所有可能的明文加密直到与截获的密文一致为止

安全性

- 无条件安全
- 计算上安全
 - 破译密码成本超过信息价值
 - 破译时间超过信息有效生命周期

密码算法

- 受限算法

保密性基于对算法的保密

- 基于密钥算法

保密性基于对密钥的保密

密码算法公开

- Make it feasible for widespread use 便于广泛使用
 - Low-cost chip implementations 低成本晶片实现
 - Maintaining the secrecy of the key 密钥的管理
-

Caesar Cipher (恺撒密码 Julius Caesar)

- replaces each letter by 3rd letter by defining transformation as:

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																		

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																		

example:

meet me after the toga party

PHHW PH DIWHU WKH WRJD SDUWB

恺撒密码描述

- mathematically assign each letter a number

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

then we have Caesar cipher as:

密文: $c = E(p) = (p + 3) \bmod 26$

解密: $p = D(c) = (c - 3) \bmod 26$

推广: 如果将移位3 推广到任意数K [1, 25], 则

$$c = E(p) = (p + k) \bmod 26$$

$$p = D(c) = (c - k) \bmod 26$$

KEY	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vgic rctva
2	nffu nf bgufs uif uphb qbsuz
3	meet me after the toqa party
4	ldds ld zesdq sqd snfz ozqsx
5	kccr kc ydrcc rfc rmey nyprw
6	jbbq jb xcqbo qeb qldx mxoqv
7	iaap ia wbpan pda pkcw lwnpu
8	hzzo hz vaozm ocz ojbv kvmot
9	qyyn qy uznyl nby niau julns
10	fxxm fx tymxk max mhzt itkmr
11	ewwl ew sxlwj lzw lgys hsjlq
12	dvvk dv rwkvi kyv kfxr grikp
13	cuuj cu qvjuh jxu jewq fqhjo
14	btti bt puitq iwt idvp epqin
15	assh as othsf hvs hcuo dofhm
16	zrrg zr nscre gur gbtn cnegl
17	yqqf yq mrfqd ftq fasm bmdfk
18	xppe xp lqepc esp ezrl alcej
19	wood wo kpdob dro dyqk zkbdi
20	vnnc vn jocna cqn cxpj yjach
21	ummb um inbmz bpm bwoi xizbg
22	tlla tl hmaly aol avnh whyaf
23	skkz sk qlzkx znk zumq vqxze
24	rjjv rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevxc

攻击手段：

1. 算法简单，密钥K的数量仅为25个
 - » 强力攻击
2. 明文单词构造有规律，可以根据字母频率
 - » 分析攻击

Figure 2.3 Brute-Force Cryptanalysis of Caesar Cipher

Rail Fence (栅栏) cipher

原文: meet me after the toga party

write message out as:

m e m a t r h t g p r y
W
e t e f e t e o a a t

密文ciphertext:

MEMATRHTGPRYETEFETEOAAT

列置换

密钥:列的读出顺序。

算法: 以一个矩阵形式逐行写出明文,
再逐列读出该消息, 并以行的顺序排列

■ 密钥: 4 3 1 2 5 6 7

明文:

a	t	t	a	c	k	p
o	s	t	p	o	n	e
d	u	n	t	i	l	t
w	o	a	m	x	y	z

密文:TTNAAPMTSUOAODWCOIXKNLYPETZ

使用多轮置换加密提高安全性

密钥: 4 3 1 2 5 6 7

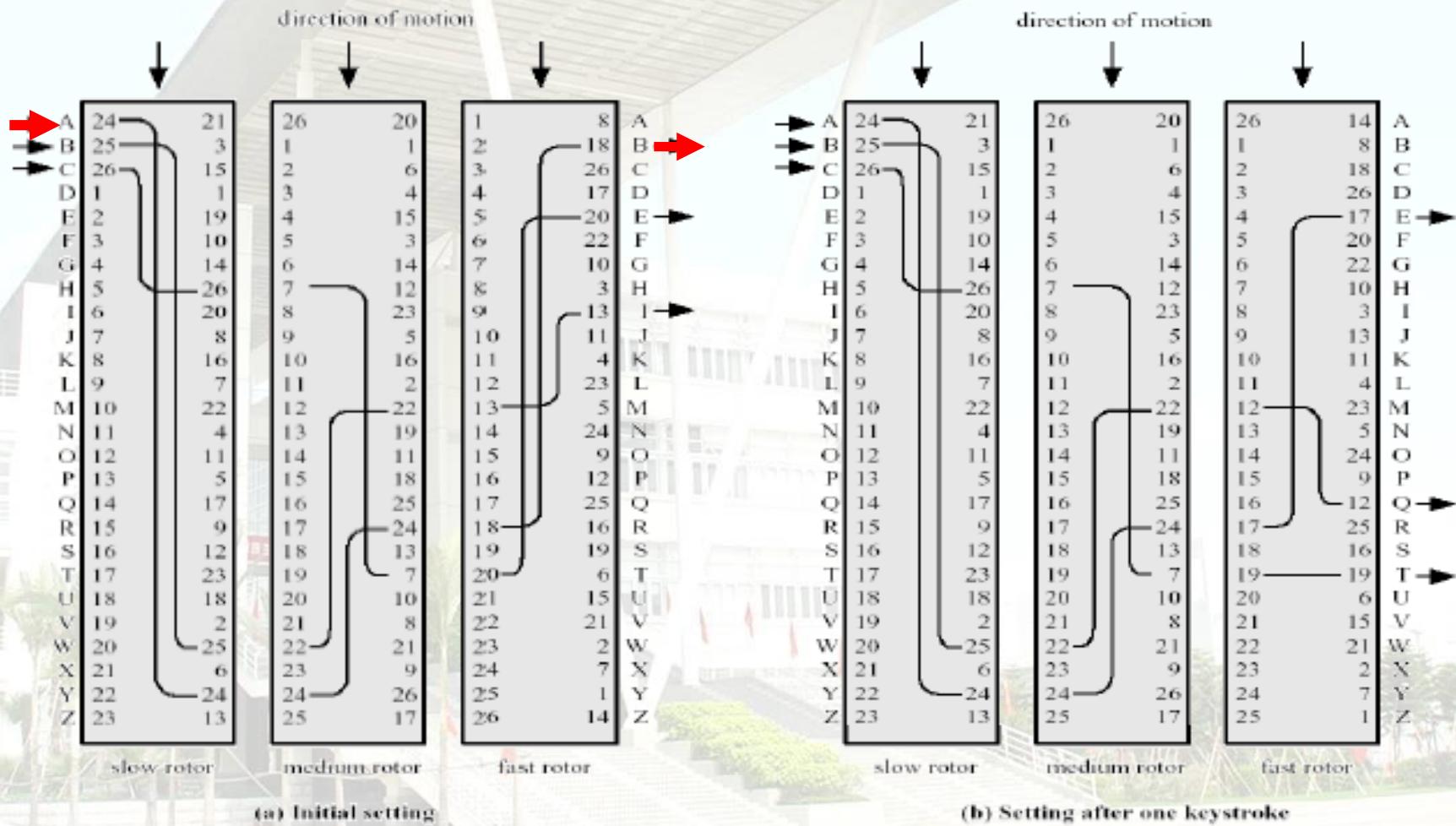
t	t	n	a	a	p	t
m	t	s	u	o	a	o
d	w	c	o	l	x	k
n	l	y	p	e	t	z

密文:

NSCYAUOPTTWLTMDNAOIEPAXTTOKZ

Rotor machine 转子机

■通过多个转子，完成字母的多次转换。



哈格林转子机 (Hagelin Rotor Machine)

)

3 cylinders

$26^3 = 17576$ 字母
替换字母表

第二次世界大战



密码学基础-安全服务原理

- 数据加解密原理-保密服务
 - 密钥管理
 - 完整性校验技术与散列演算法-检验服务
 - 数字签名（**Digital signature**）技术-签名服务
-

安全机制

可逆： 加密解密



不可逆：

HASH

MAC

Digest,

Digital Signature

Authentication

消息

SHA256

256 - bit 数据

密码编码

1) 明密转换类型:

- 替代 : 明文中的元素映射成另一元素。
- 置换 : 明文中的元素被重新排列。

2) 密钥数量: 单密钥/ 双密钥

3) 明文处理方式: 分组(block) /流(stream)

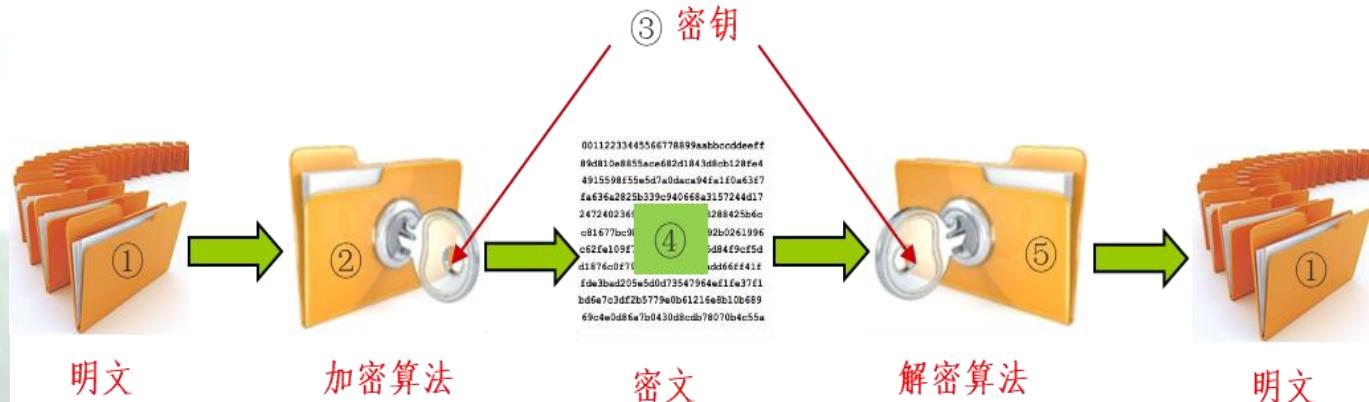


对称密码算法:单密钥

非对称密码(公钥)算法:双密钥

对称加密算法 (Symmetric Encryption)

- 加密运算与解密运算使用同一把密钥，对称密码模型如图



注： ③ 密钥=加密密钥=解密密钥， 加密算法②=解密算法⑤

- ✓ 由5部分组成：①明文、②加密算法、③密钥、④密文、⑤解密算法
- ✓ 加密算法与解密算法采用同一算法，加密密钥与解密密钥为同一把密钥
- ✓ 常见的对称加密算法有AES、3DES、以及SM4

对称密码算法优缺点

□ 对称加密的优点

- 速度快, 处理量大, 适用: 数据的直接加密
- 加密密钥长度相对较短, 128-bit, 256-bit, 512-bit

□ 对称加密的缺点

- 密钥双方一致、保密, 传递较难
- 大型分布网路中密钥量大, 难以管理, 一般需要KDC
(Key Distribution Center)
- 密钥需要经常更换

非对称密码算法

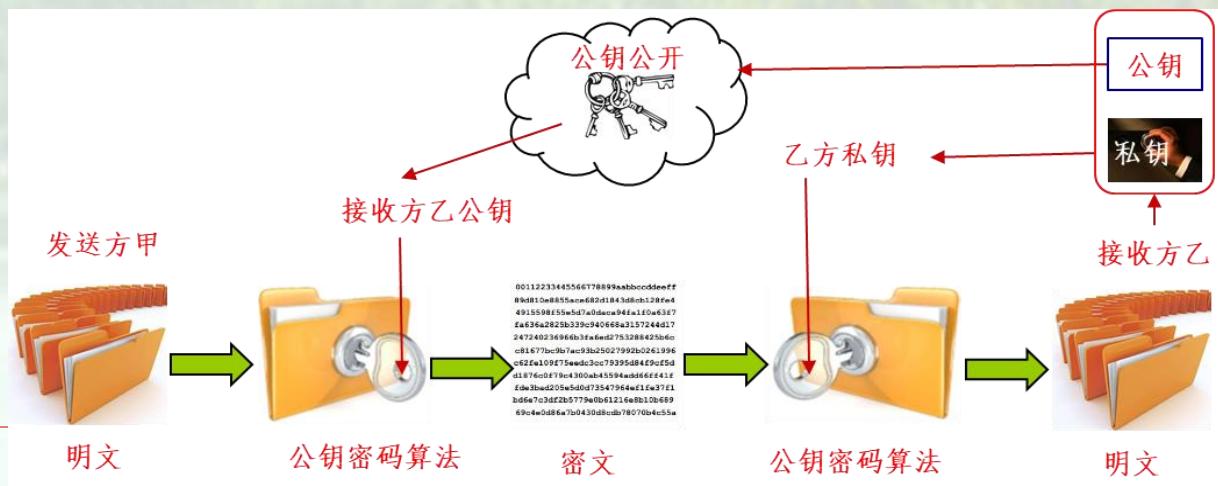
每个实体产生一对密钥

- 具有两把不同密钥，一把称为公钥（Public-Key）
一把称为私钥（Private-key）
- 任何一把都可用于加密，而另外一把则用作解密
- 特点
- ✓ 用公钥加密的数据只能用私钥解密，而用私钥加密的数据只能用公钥解密
- ✓ 公钥公开存放/发布，以供访问获取，所有的人或实体都可得到它
- ✓ 私钥是私有的，不应被其他人或实体得到，且保持机密性



非对称密码算法模型

- 非对称密码模型包括：明文、加密算法、公钥、私钥、密文、解密算法
- 常见非对称加密算法有RSA，ECC，以及SM2
- 特点
 - ✓ 仅根据公开密码算法和加密密钥来确定解密密钥在计算上是不可行的
 - ✓ 两把密钥中的任何一把可用来加密，另一把则用来解密，但作用则不同

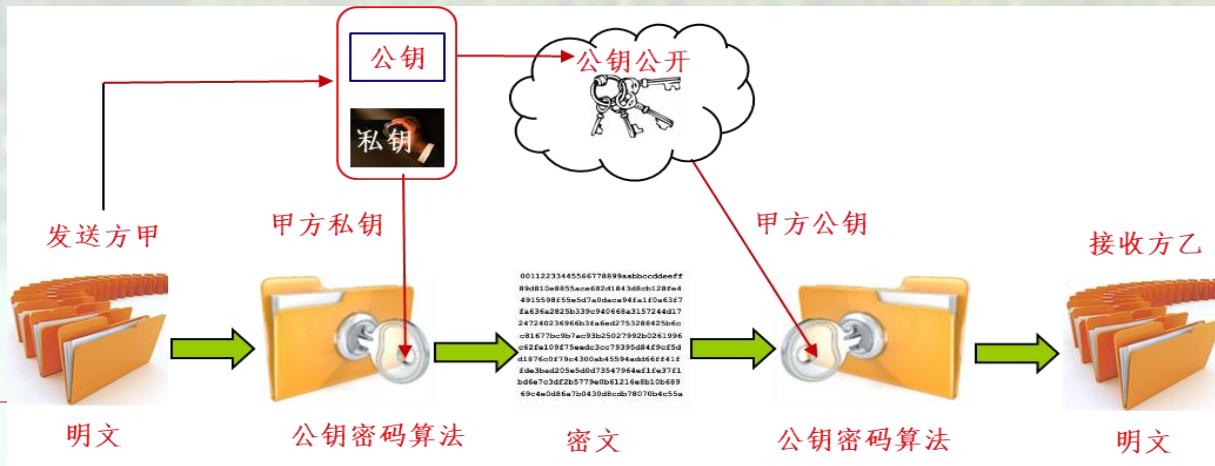


保密模型

非对称密码算法-鉴别模型

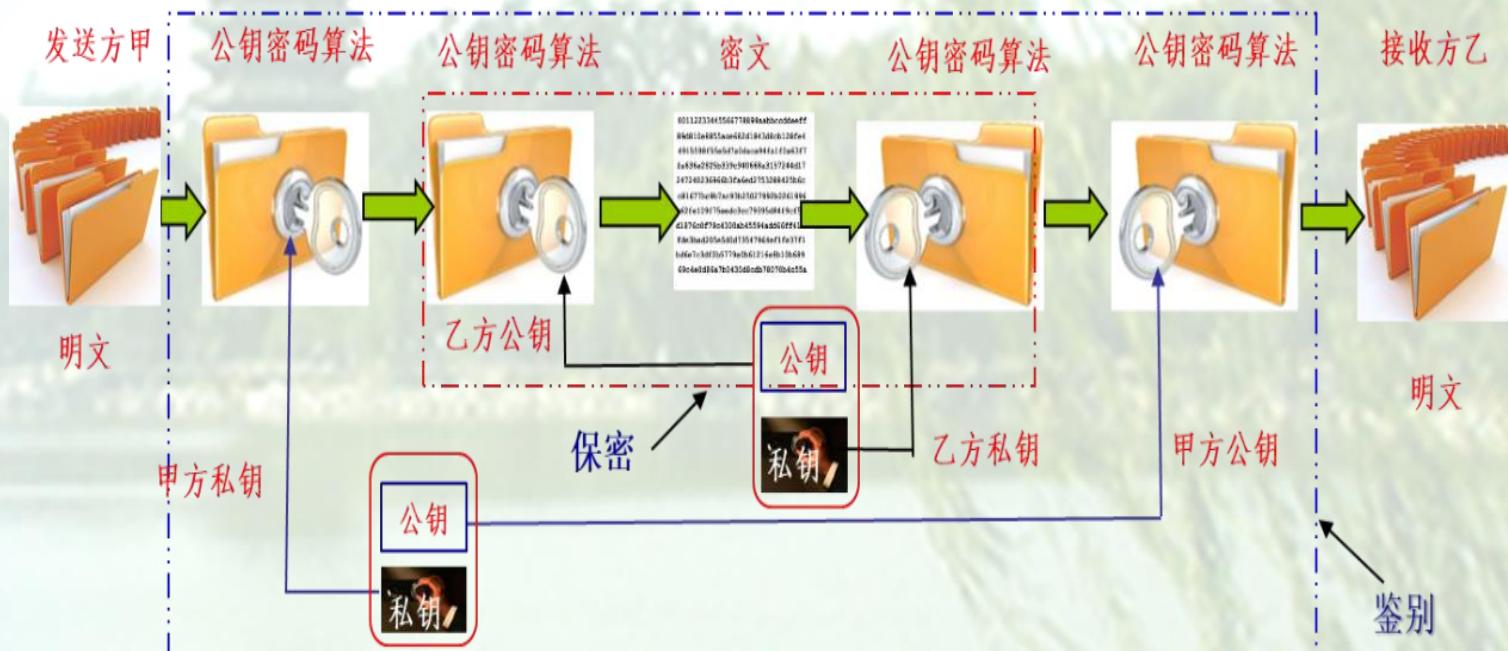
➤ 工作原理

- ✓ 发送方甲想发数据给接收方乙，则用甲方**A**的私钥对数据进行加密，乙方**B**只用**A**的公钥才能对数据进行解密得到原数据
- ✓ 所有实体只要能从公开网路获得**A**的公钥，都能用**A**的公钥对数据进行解密得到原数据，因此该模型只用于鉴别数据来源于甲方**A**，即验证了该数据由甲方**A**签发，但并没有对该数据进行保密。



具有保密和鉴别功能的公开密码模型

- 为了同时提供数据的机密性以及鉴别性，则需要先用发送方甲A的私钥进行加密完成签名，再用接收方乙B的公钥对整个消息进行加密。
- 代价是每次要执行四次比对称密码算法费时得多的公开密钥密码算法



完整性校验技术与散列算法-检验服务

➤ 数据完整性

- ✓ 用于评测数据在存储、传输、交互以及分享等各环节中，数据是否部分损坏丢失或被篡改

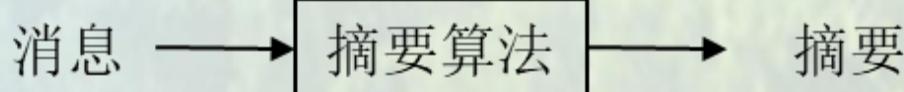
 - ✓ 目的
确保数据在整个生命周期各环节中的一致性

 - ✓ 完整性校验技术是网路通信技术的重要支撑技术，更是数字签名、及区块链的核心算法基础
-

消息摘要演算法模型

消息摘要（Message Digest）算法也称为数字摘要(Digital Digest) 算法

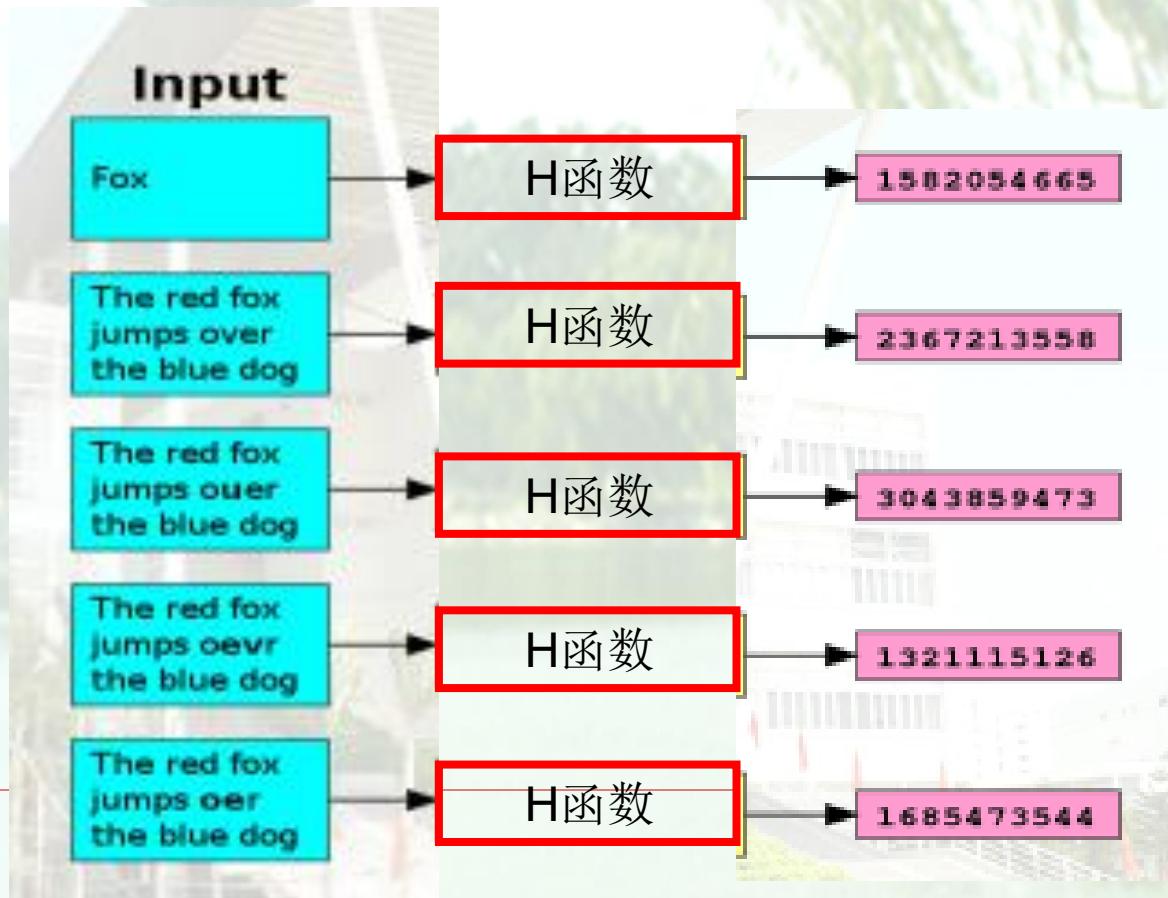
- 把任意长的输入消息串变化成固定长的输出串的函数，是一个单向函数，消息的转化是一个不可逆的过程，如图所示



- 构造两个不同的消息，将它们映射为同个消息的摘要计算上不可行的

把任意长输入串变化成固定长的输出

消息任何一位或多位的变化将导致输出值的变化



H函数与“碰撞”

- 输入为任意长度的消息；
 输出为一个固定长度值，
 - 构造两个不同的消息，将它们映射为同个消息的摘要计算上不可行的
-
- ✓ 如果内容不同的明文，通过H算法得出的结果相同，就称为发生了“碰撞”
 - ✓ 算法的用途不是对明文加密，让别人看不懂，而是通过对信息摘要的比对，防止对原文的篡改
 希望碰撞率要低

碰撞

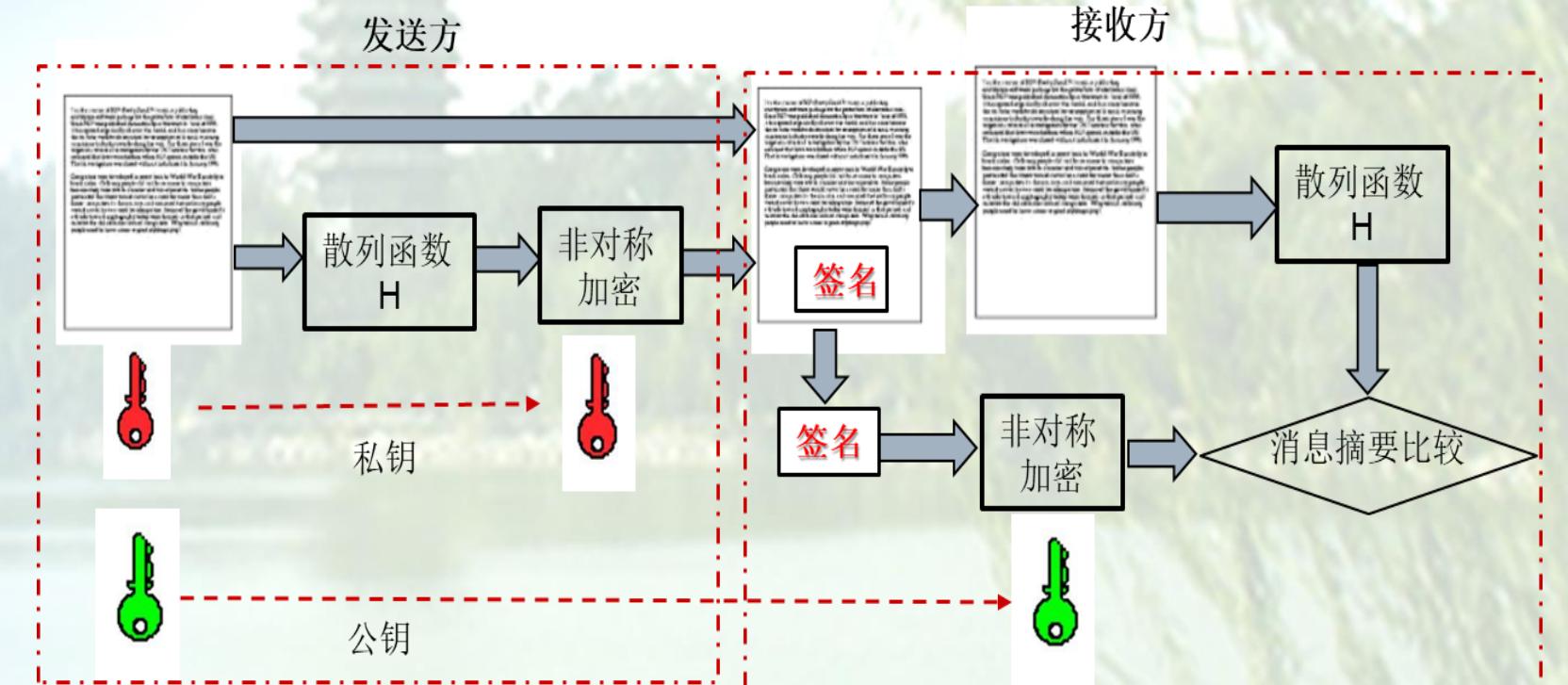
理论上说，当这种摘要算法被完全攻破时，也就是说可以从摘要恢复出任意原文

注意：是任意原文，因为所有的摘要算法的特点就是存在着一个无穷大的碰撞原文的集合。而真正的原文只是其中一份。

对应这个无穷大的集合来说，这就是可能性无穷小

数字签名（Digital signature）技术

目的是为了保证信息传输过程的完整性、防止信息交互中发生抵赖，即防止发送方否认已发送报文、及接收方伪造报文。



Digital Signature



This is the creation of RSA. Every digital signature is a two-step process. First, the message is hashed. Then the hash is encrypted with the private key. Since the private key is unique to each user, the hash is unique to each user.

Encryption was first developed in World War II to encode messages sent over radio. Only very powerful and expensive computers were available at the time. So the message had to be broken down into smaller pieces and then each small section had to be encoded by hand. This was a slow process. By the time it was completed, the message had been decrypted by the enemy. So the message had to be re-encoded and sent again. This process was very slow and took a lot of energy.



This is the creation of RSA. Every digital signature is a two-step process. First, the message is hashed. Then the hash is encrypted with the private key. Since the private key is unique to each user, the hash is unique to each user.

Encryption was first developed in World War II to encode messages sent over radio. Only very powerful and expensive computers were available at the time. So the message had to be broken down into smaller pieces and then each small section had to be encoded by hand. This was a slow process. By the time it was completed, the message had been decrypted by the enemy. So the message had to be re-encoded and sent again. This process was very slow and took a lot of energy.

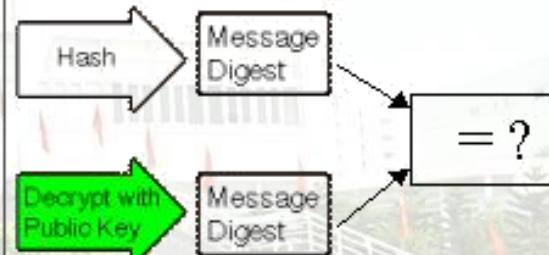
Signature



This is the creation of RSA. Every digital signature is a two-step process. First, the message is hashed. Then the hash is encrypted with the private key. Since the private key is unique to each user, the hash is unique to each user.

Encryption was first developed in World War II to encode messages sent over radio. Only very powerful and expensive computers were available at the time. So the message had to be broken down into smaller pieces and then each small section had to be encoded by hand. This was a slow process. By the time it was completed, the message had been decrypted by the enemy. So the message had to be re-encoded and sent again. This process was very slow and took a lot of energy.

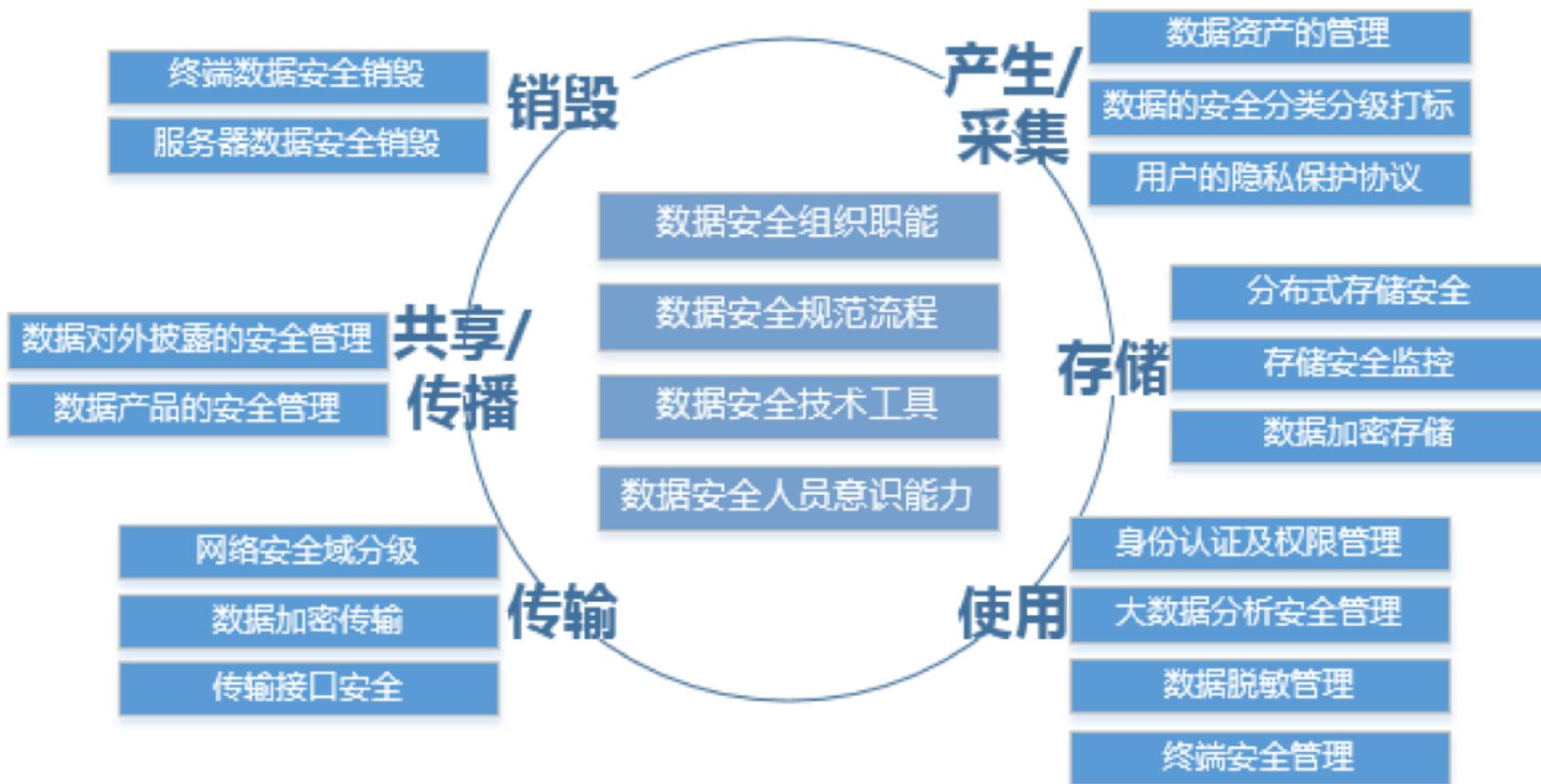
Signature



覆盖数据全生命周期的数据安全防护体系

- 在移动计算、云计算及智能分析的环境下，数据在采集、传输、存储、挖掘、分析、处理、交互、共用及服务各环节可能出现的数据安全问题，上下游产业在数据安全管理及隐私保护等
- 覆盖数据全生命周期的数据安全防护体系，以及支撑该体系关键技术，包括授权、鉴权、密钥共享、加密、脱敏、抗抵赖等数据安全及隐私保护技术。

围绕数据生命周期的大数据安全实践



各行各业的大数据安全实践融合

□ 联邦学习 (Federated Learning)

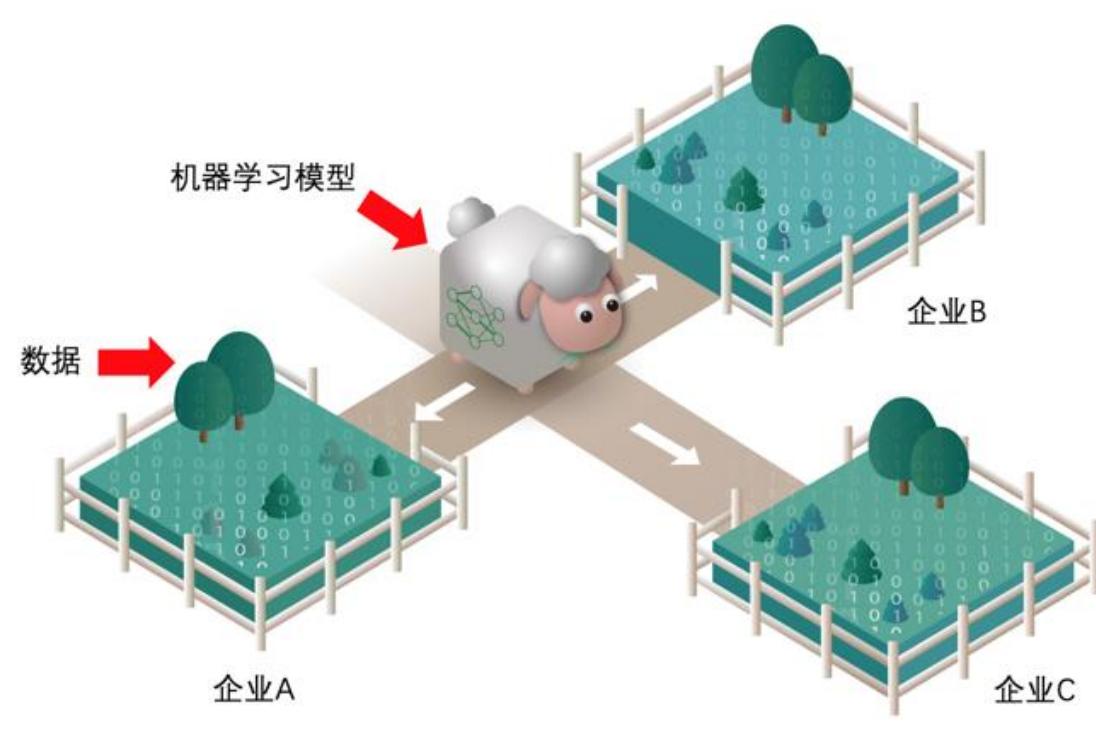
- 一种分布式机器学习技术（机器学习框架），在保证数据隐私安全及合法合规的基础上，实现共同建模，提升**AI**模型性能

数据不动

模型动

数据可用

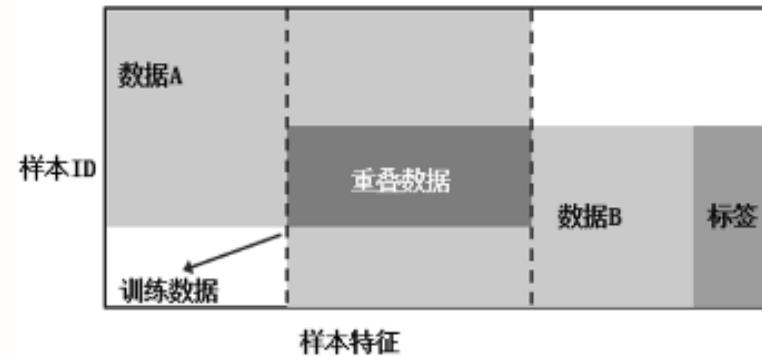
不可见



原始数据和模型私密参数数据都不动和不可见

例如：横向联邦学习

Horizontal Federated Learning

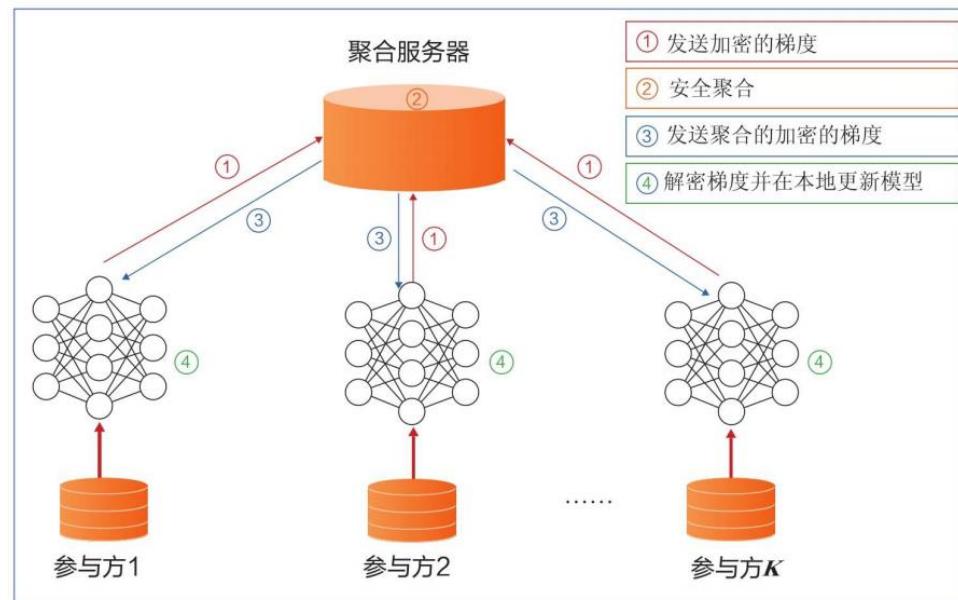


➤ 适用场景

特点是样本的联合，适用于相同业态的参与者间协同，但各自的客户不同，即特征重叠多，用户重叠少

如：不同地区银行之间，业务相似（特征相似），但用户不同（样本不同）

- ① 参与方各自从聚合服务器下载最新模型
- ② 各参与方利用本地数据训练模型，加密梯度上传给服务器，服务器聚合各用户的梯度更新模型参数
- ③ 服务器返回更新后的模型给各参与方
- ④ 各参与方更新各自模型



基于样本的分布式模型训练，各自从服务器下载模型，然后利用本地数据训练模型，然后返回给服务器更新参数；服务器聚合各机器上的返回的参数，更新模型，再把最新的模型反馈到各方；各方都用相同且完整的模型，且各方之间不交流不依赖，在预测时独立预测

智能环境下电子政务/电子商务的发展趋势与管理模式

北京大学 信息工程学院

朱跃生

2022年12月

北京大学

电子政务

Electronic Government

G2G：政府间电子政务

G2B：政府-商业机构间电子政务

G2C：政府-公民间电子政务

G2E：政府-雇员间电子政务

➤ 联合国

利用信息通信技术手段，密集性和战略性组织政府管理方式

- ✓ 提高政府管理效率
- ✓ 增强政府的透明度
- ✓ 改善财政约束
- ✓ 改进公共政策品质和决策的科学性
- ✓ 建立良好的政府间、政府与社会、社区以及政府与公民间关系
- ✓ 提高公共服务品质，赢得广泛社会参与度

➤ 世界银行

利用信息技术，赋予政府部门独特能力，转变其与公民、企业、政府部门间关系

- ✓ 向公民提供更有效的政府服务
- ✓ 改进政府与企业和产业界关系
- ✓ 更好地履行公民权
- ✓ 增加政府管理效能
- ✓ 减少腐败
- ✓ 提供透明度
- ✓ 促进政府服务便利化
- ✓ 增加政府收益或减少政府运行成本

需求

城市发展及管理新思维，通过推进城市生产、生活和管理方式创新，改善提升政府服务水准、创造产业经济价值、提升民众生活水准

智慧城市 达到 “**优政、兴业、惠民**” 目标

- 城市基础设施(水、电、气、管线)
- 信息网路基础设施
- 智能建筑
- 智能交通
- 电子政务
- 公共安全与应急
- 环境保护
-

城市建设：
解决城市发展问题

产业发展：
加快经济转型升级

人民生活：
提高人民生活质量

- 智能工业
- 现代农业
- 智能物流
- 金融
- 电子商务
- 现代服务业
-

- 智能旅游
- 智能医疗
- 智能教育
- 智能家居
- 社区服务
- 食品安全
- 文化生活
-

智慧城市建设

公共服务便捷化

建立跨部门跨地区业务协同、共建共用的公共服务信息服务体系
利用信息技术，创新发展城市教育、就业、社保、养老、医疗和文化的服务模式

产业发展现代化

传统产业信息化改造，推进制造模式向数字化、网路化、智能化、服务化转变

发展信息服务业，推动电子商务和物流信息化集成发展，创新并培育新型业态

社会治理精细化

市场监管、环境监管、信用服务、应急保障、治安防控、公共安全等社会治理领域，建立完善相关信息服务体系，创新社会治理方式

城市建设及管理发展趋势

- **统筹城市发展的物质资源、信息资源和智力资源利用**
- **推动物联网、云计算、大数据、人工智能等新一代信息技术创新应用，实现与城市经济社会发展深度融合**
- **强化信息网路、信息中心等信息基础设施建设**
- **促进跨部门、跨行业、跨地区的政务信息共用和业务协同，强化信息资源社会化开发利用，推广智能化信息应用和新型信息服务，促进城市规划管理信息化、基础设施智能化、公共服务便捷化、产业发展现代化、社会治理精细化。**
- **增强城市要害信息系统和关键信息资源的安全保障能力**

智慧城市内涵

- 建立在物联网、互联网、云计算、大数据分析、遥感遥测、人工智能等新一代信息技术基础上
 - 带来研发、生产、管理、服务效率的提高
 - 打破时空限制，实现生产生活要素有机组合
-
- ◆ 城市公共服务资源向乡镇延伸和覆盖
 - ◆ 城市管理更加科学
 - ◆ 人居环境更加优美
 - ◆ 产业结构更加高效
 - ◆ 城乡发展更加均衡



城市管理内涵

- 人地（地理环境）关系系统，体现人与人、地与地、人与地相互作用和相互关系
- 由政府、企业、市民、地理环境等，既相对独立又密切相关的子系统构成
- 体现政府管理、企业的运营、市民的生活间的人地关系
- 城市信息化
充分体现“人”的主导地位，更好地把握城市系统的运动状态和规律，对城市人地关系进行调控，实现系统优化，有利于可持续发展

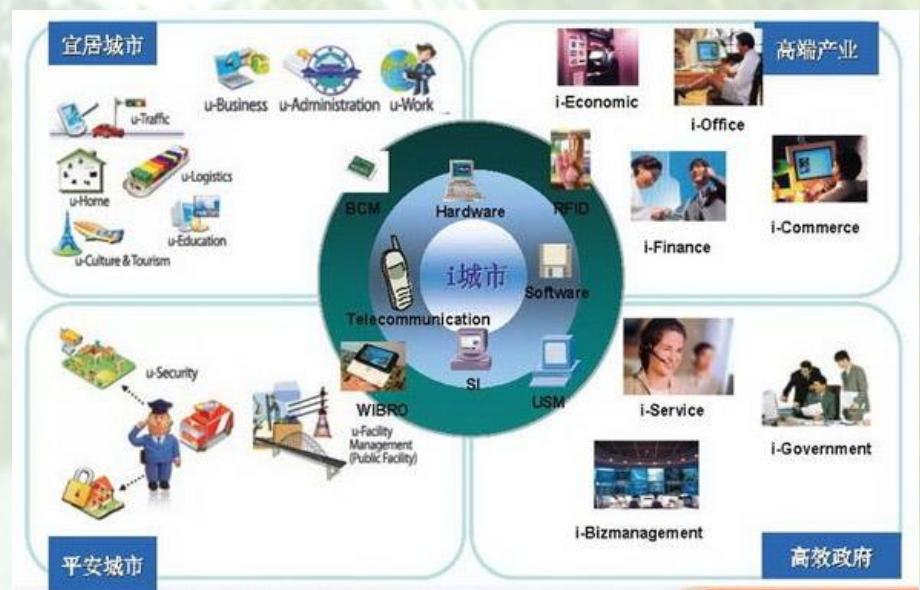


智能环境下电子政务创新



在智慧数字应用

- 信息：全面感知，可靠传递，安全存储，智能处理，启示利用
- ✓ 全面收集（历史），动态获取（现在），预测启示（将来）
- 智慧城市面向应用和服务
- 智慧城市与物理城市融为一体
- 实现自主组网、自维护
- 智慧民生服务



北京大学

政府及公共大数据

□ 政府所拥有和管理的数据

公安、交通、医疗、卫生、就业、社保、地理、文化、教育、科技、环境、金融、统计、气象等数据

数据获取通常由政府下属机构或事业单位通过网路与政府信息中心交互传送

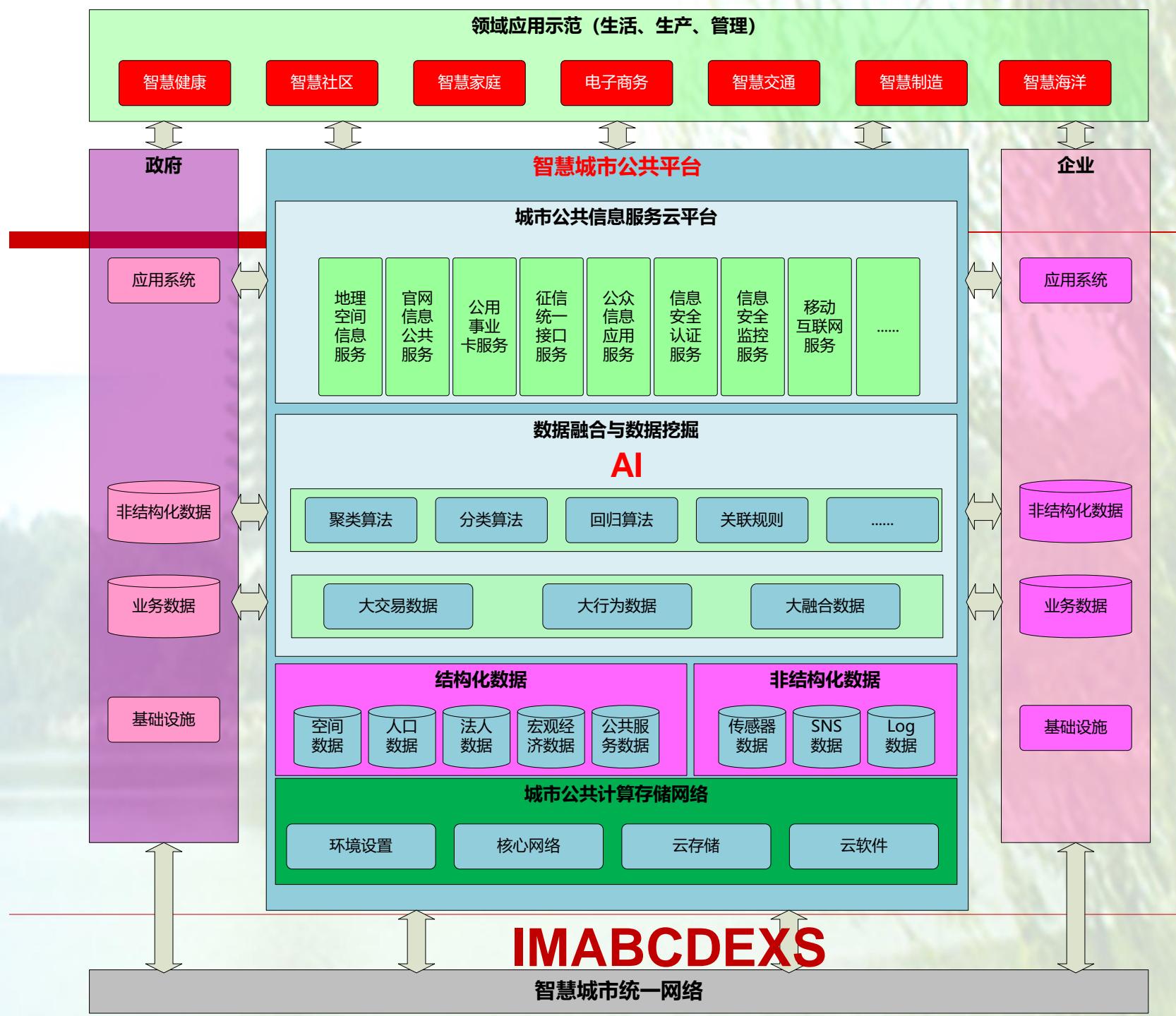
□ 因管理服务需要而采集的外部大数据

互联网舆论等数据

或直接存放在分支机构中

□ 一般分五类

- (1) 拥有政府资源权利才有可能采集的数据
如税收类、财政类等数据
- (2) 利用政府资源许可权才有可能汇总或获取的数据
如建设类、农业类、工业类等数据
- (3) 事业单位产生的数据
如城市建筑、交通设施管理、医院**HIS**系统管理、教育资源及管理等数据
- (4) 政府监管职责所拥有的数据
~~如人口普查、食品药品管理等数据~~
- (5) 政府部门提供服务的数据：
如社保、水电、教育信息、医疗信息、交通路况、公安等数据



我国电子政务发展趋势

➤ 数字政府

- ✓ 整体带动和提升数字中国建设
- ✓ 数字经济、数字社会、数字文化及数字生态的核心结合部
- ✓ 向数据共享、业务协同的方向转变，促进政府决策科学化、社会治理精准化、市场监管高效化

➤ 公共服务

政府信息化建设发展重点转向提高公共服务能力

➤ 移动政务

移动互联网发展大势所趋

➤ 政务数据治理和信息整合共享

整合“数字碎片”、打破“信息孤岛”、拆除“数据烟囱”，实现政务信息资源高效流动，全面推进政务信息资源共享和业务协同

电子政务发展趋势（2）

- **自主可控核心技术产品创新升级**
- **新技术应用融合**
- ✓ **大数据、云计算、区块链、人工智能，移动计算等新信息技术将在电子政务服务中扮演重要角色，推动政务资源整合、优化政务流程，提升政府服务质量和效率，促进国家治理体系与治理能力现代化**
- ◆ AI**将成为电子政务发展方向**，以深度学习、机器学习为特征，成为提高政府治理能力和公共服务能力的重要驱动力
- ◆ AI**将广泛应用于政府大数据采集、加工处理、分析挖掘、智能服务等环节**，通过**高效采集、有效整合**、充分运用政府数据和社会数据，推动电子政务服务从数字化、网络化向**智能化发展**。



互联网服务和商业模式演进带来的思考

✓ 互联网门户时代
Yahoo!

✓ 搜索时代
Google, 百度

✓ 移动互联网时代
Apple, 三星, 华为, 小米等智慧终端机

✓ 社交网路时代
微信, Facebook, Twitter, 人人网…

✓ 互联网消费时代
亚马逊, eBay, 淘宝, 京东…



电子商务

电子商务

Electronic Commerce

- 以信息网路技术为手段，以商品交换为中心的商务活动；以电子交易方式进行交易活动和相关服务的活动，将传统商业活动各环节电子化、网络化、信息化的商业行为
- 在开放的网路环境下，实现消费者网上购物、商户间网上交易和线上电子支付以及各种商务活动、交易活动、金融活动等相关综合服务活动的商业运营模式

ABC (代理商、商家和消费者 Agent、Business、Consumer)

B2B (企业对企业 Business-to-Business)

B2C (企业对消费者 Business-to-Consumer)

C2C (个体对消费者 Consumer-to-Consumer)

C2B (消费者对企业 Consumer-to-Business) 、

B2G (企业对政府 Business-to-Government)

C2G (消费者对政府 Consumer to Government)

O2O (线上对线下 Online To Offline)

M2C (Manufacturers to Consumer 生产厂家对消费者)

B2M (Business to Marketing 企业对市场营销)

EC发展阶段

□第一阶段

电子邮件，70年代开始

□第二阶段

信息发布，从1995年起，以Web技术为代表的信息发布系统，成为Internet的一种主要应用

□第三阶段

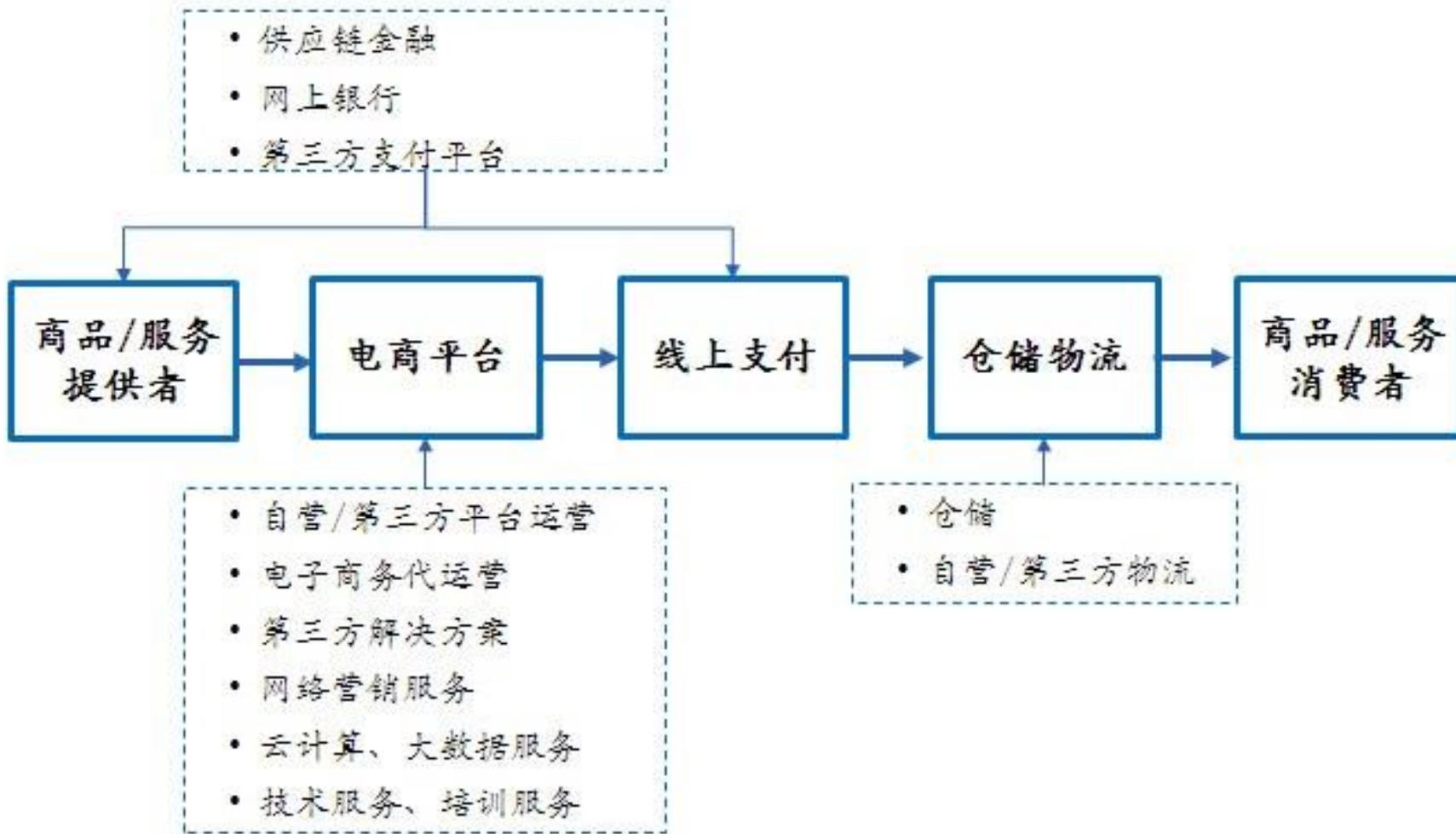
正式进入EC电子商务阶段，1997年由美加发起，1998年为电子商务年

□第四阶段

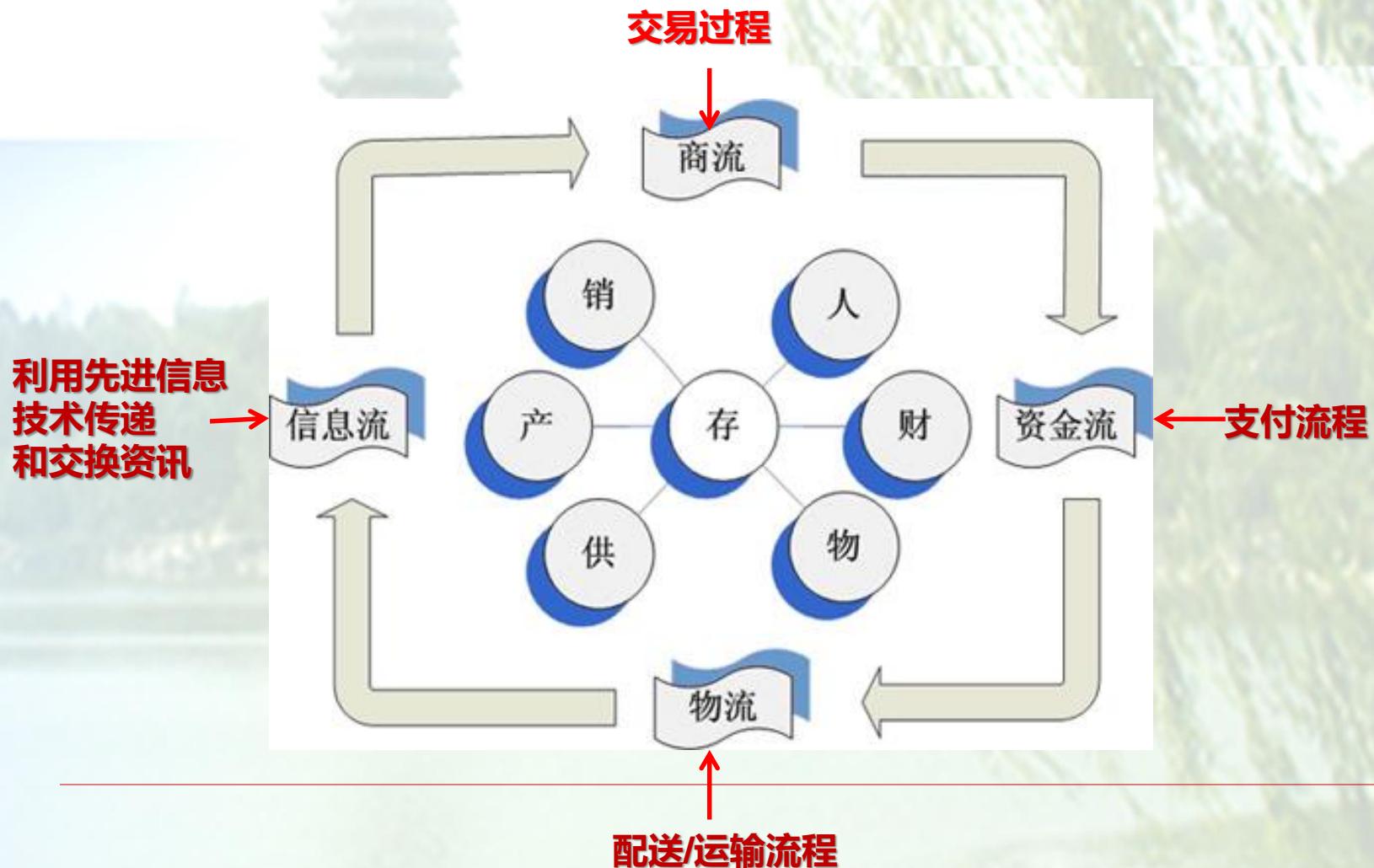
全程电子商务，在云计算的支持下形成电子商务产业链条

□第五阶段

目前开始的智能阶段



促进商流、物流、资金流和信息流融合发展



云电子商务 (Cloud e-Commerce)

➤ 基于云计算的电子商务平台服务

电子商务产业链

供应商
代理商
策划服务商
制造商
储运商
行业协会
管理机构
行业媒体
法律结构



资源间相互展示和互动
按需交流
达成意向

降低成本
提高效率

云平台与服务



阿里云



数字信封 (Digital Envelope)

保证只有规定的特定收信人才能阅读信的内容：

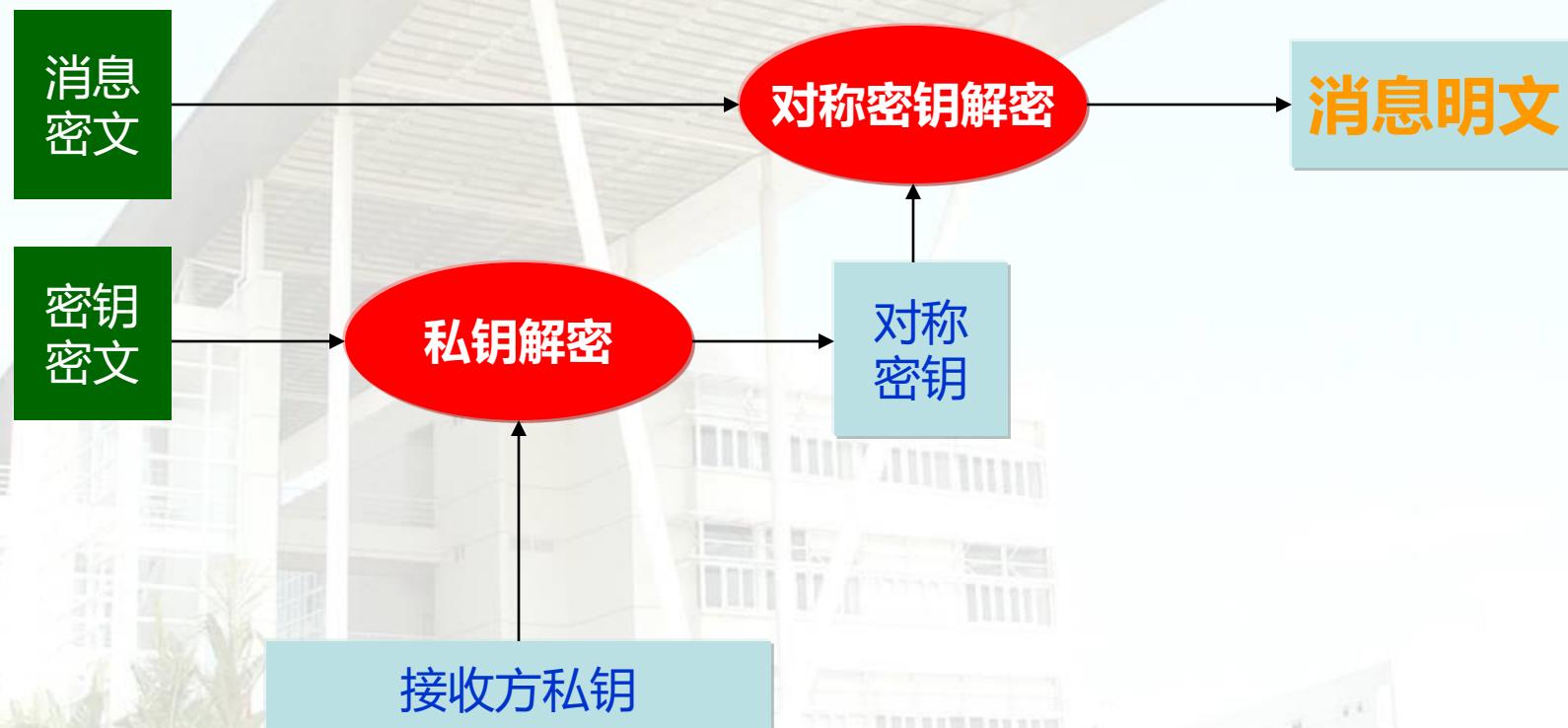
数字信封的生成：

- 发送方用**对称密钥加密信息**
- 发送端用**接收端的公钥**，将**对称密钥加密**，生成一个**数字信封**
- **接收端用自己的私钥**打开**数字信封**，**获取该对称密钥**，用它来**解读收到的信息**

数字信封的生成



数字信封的解读



双重数字签名在EC的应用

实现三方通信时的身份认证和信息完整性、防抵赖的保护

- 发送者寄出两个相关信息给接收者，对这两组相关信息，接收者只能解读其中一组，另一组只能转送给协力厂商接收者，不能打开看其内容。这时发送者就需分别加密两组密文，做两组数字签名。
- 网上购物：
客户和商家之间要完成线上付款，在客户A、商家B和银行C之间将面临以下问题：
A向B发送订单和A的付款信息；
B收到订单后，要同C交互，以实现资金转账。
A不愿让B看到自己的帐号信息，也不愿让C看到订购信息。
A使用双重签名技术对两种信息作数字签章，来完成以上功能。

双重数字签名的实现（1）

- A对发给B的信息 M_B 生成摘要 H_{MB} ；
- A对发给C的信息 M_C 生成摘要 H_{MC} ；
- A把 H_{MB} 和 H_{MC} 合起来生成摘要 H_{MBC} ，
并用私钥签名 H_{MBC} —» $Sig(H_{MBC})$ ；
- A把 M_B 、 H_{MC} 和 $Sig(H_{MBC})$ ； —» B；
- A把 M_C 、 H_{MB} 和 $Sig(H_{MBC})$ ； —» C；

双重数字签名的实现（续）

- B 接收信息后，对 M_B 、生成信息摘要 H_{MB}' ，把 H_{MB}' 和收到的 H_{MC} 合在一起，生成新的信息摘要，同时使用A的公钥对签名 $Sig(H_{MBC})$ 进行验证，确认信息发送者的身份和信息是否被修改？
- C接收信息后，对 M_C 生成信息摘要 H_{MC}' ，把 H_{MC}' 和收到的 H_{MB} 合在一起，并生成新的信息摘要，同时使用A的公钥对对签名 $Sig(H_{MBC})$ 进行验证，确认信息发送者的身份和信息是否被修改？