谈谈密码研究从黑屋子走向民间后的革命效应

翟起滨

qibinzhai@ucas.ac.cn

中国科学院信息安全国家重点实验室

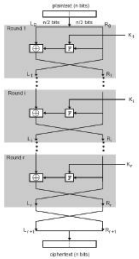
2017年9月22日西安

朝鲜战争刚结束,美国军方干了两件大事

1.成立了国家安全局(NSA)，从大学里调进一大批优秀的专家和教授；
2.建立军民融合(Civil-Military Integration)的特别机构-国防部高级研究计划署(Defence Advanced Research Projects Agency)简记为DARPA,它的使命是推动技术创新，使美国的国防技术总是领先其它国家。这个机构促进美国军方积极向民间公司提出军用项目的需求,并且大量采购相应的产品。IBM、Intel、AT&T等民间公司,在上世纪60年代初参与了这个高级研究计划署DARPA的计算机网络项目，到1969年建立起ARPA网络,这正是Internet的雏型。网络很快推向学校和科研机构，利用网络通讯进行交流成为十分方便的形式。

上世纪70年代初IBM得到英国金融和保险业关于有保密功能的计算设备订单，NSA帮助IBM设计商用密码，于是密码从美国军方流向民间！

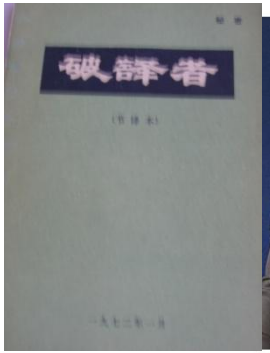
DES – U.S. Data Encryption Standard (1976)

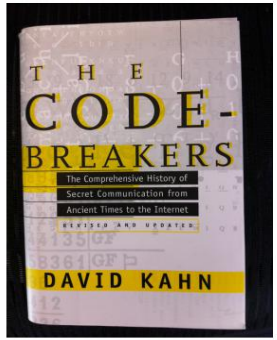


DES Designed at IBM; Horst Feistel supplied key elements of design, such as ladder structure. NSA helped, in return for keeping key size at 56 bits.(?)

“中国民间的力量不可估量！”

Kahn – The Codebreakers





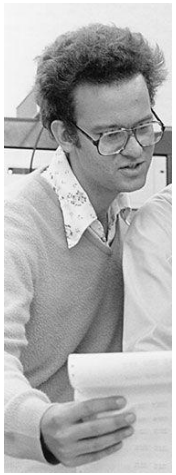
In 1967 David Kahn published
The Codebreakers—The Story of Secret Writing.
A monumental history of cryptography.
NSA attempted to suppress its publication.

美国的大学师生开始公开研究密码学问题，

信息革命的火种在美国点燃！

20岁出头的Ralph Merkle给出在不安全的信道上商议新的加密密钥方法

当时困扰网络专家的头等问题就是通信双方如何在不安全的信道上商议 ‘密钥”



●1974年秋季，Ralph Merkle在加州大学伯克力分校选修 Lance Hoffman教授开设的计算机安全课程，Merkle提出的选题是“不安全网络上的安全通信”，试图解决通信双方的密钥交换问题。Hoffman不理解，让他重选，他不干！他退选了课程，写出研究论文《多用户加密技术》投搞ACM的通讯杂志，被退稿！

●1975年秋季，斯坦福大学 ：数学博士Diffie 和电机系教授Hellman应邀 为1976年的美国计算机会议撰写论文，这期间他们收到了Merkle被拒的论文。Diffie和Hellman收到Merkle的文章后深受启发，建立数学模型写出了划时代的论文：密码学的新方向！

信息革命的实践

信息革命的先锋用 “数学”点燃了用以前进的明灯,1976年11月D-H公开发表“密码学的新方向”,数学家Whit Diffie 起了最关键的作用,因为他用数学理论清晰地把所解决的问题表达出来,让人心服口服!

Invention of Public Key Cryptography

- Ralph Merkle, and independently Marty Hellman and Whit Diffie, invented the notion of *public-key cryptography*.
- In November 1976, Diffie and Hellman published *New Directions in Cryptography*, proclaiming

  “We are at the brink of a revolution in cryptography.”

Nov. 1976: The Diffie-Hellman System

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

New Ideas:

- Key Exchange
- Public Key Encryption
- Digital Signatures
- Code Obfuscation
- One way functions
- Trapdoor functions

W E
cr
hardwar
chanical

olution in
ap digital
ons of me-
igh grade

I.

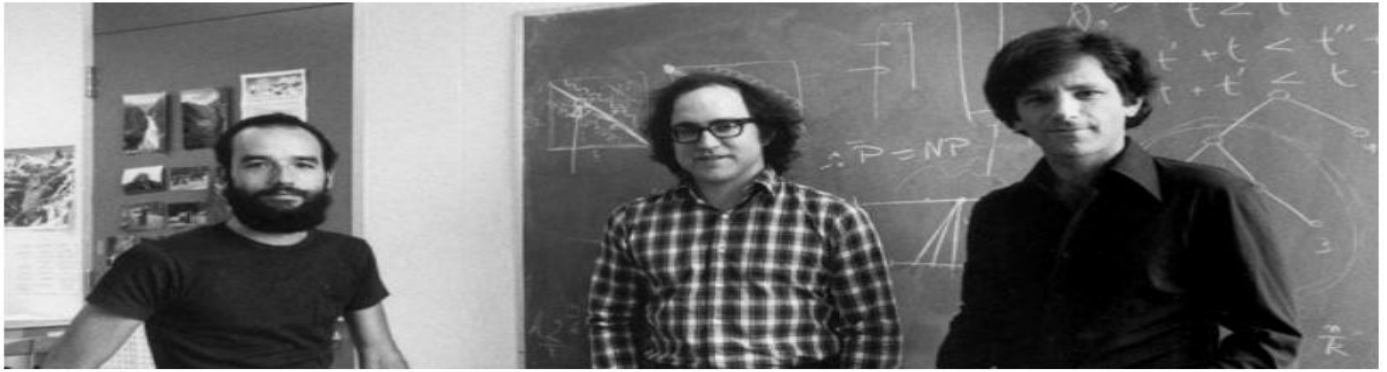
W E STAND TO
cryptography.
hardware has freed it
chanical computing and brought the cost of high grade
cryptographic devices down to where they can be used in

or acquaintance is a com
wever, and it is unrealisti
acts to be postponed lon
d by some physical means
by this key distributio
the transfer of busines
ocessing networks.

Section III proposes two approaches to transmittin
keying information over public (i.e., insecure) channel

带陷门的单向函数发现

RSA (Ron Rivest, Adi Shamir, Len Adleman, 1977)



- Security relies (in part) on inability to factor product n of two large primes p, q.
- $PK = (n, e)$ where $n = pq$ and $\gcd(e, \phi(n)) = 1$
- $SK = d$ where $de = 1 \mod \phi(n)$
- Encryption/decryption (or signing/verify) are simple:

$$C = PK(M) = M^e \mod n$$
$$M = SK(C) = C^d \mod n$$

Rivest, Shamir, and Adleman obtained a patent through MIT for their development, and in 1982 they set up a company in Adleman ‘s apartment. It was called RSA Data Security !

R 、S 、A三人于1977年8月在康乃尔大学报告论文时,美国NSA警告Rivest,宣读密码论文,相当于向外国出口加密技术。54年法案说明了这一点!

MIT为力挺学校老师的研究成果,成立探索改变美国现行密码政策的委员会。

U.S. cryptography policy evolves

- U.S. government initially tried to control and limit public-sector research and use of cryptography
- Attempt to chill research via ITAR (1977)
- MIT “Changing Nature of Information” Committee (1981; Dertouzos, Low, Rosenblith, Deutch,Rivest,...)

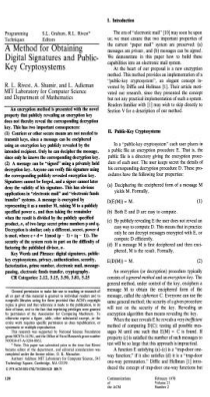
MIT Committee Seeks Cryptography Policy

Questions of who should do research on cryptography and how results should be disseminated are the first order of business

Within the next 10 years, networks consisting of tens of thousands of computers will connect businesses, corpora- quences for individuals and for society if computers continue to be connected, as they are now, according to local deci- easy to send computer programs between connected machines and to instruct a program to search for, select,

Science, 13 Mar 1981

Publication of RSA memo and paper



LCS-82 Technical Memo (April 1977)
CACM article (Feb 1978)

Public key crypto is everywhere

Internet protocols:

- SSL/TLS
- IPsec/IKE
- SSH
- S/MIME
- POP/IMAP
- DNSsec
- SBGP
- WAP

Real World:

- Online shopping
- Online banking
- Mobile communication
- Smartcards
- Email communication
  - Doctors and patients
  - Insurance Co.'s and brokers
  - Supply chain
- Protecting documents

1986年2月 Jim Bidzos, 收购了RSA数据安全公司,给出公司经营策略,打造新产品: RSAtoolket, RSAengine ,RSAbisave… ;86年6月与Lotus签署合同赚了第一笔大钱!紧接着与Motorola , Digital,Novell……,都签了大单。

●1989年2月,美国政府的计算机网络技术委员会指定RSA公司为其会员提供公钥密码产品.Bidzos坚持不断与美国政府谈判,于1990年2月,美国NSA为RSA加密软件颁发了许可证。

● 1991年11月Bidzos发起了一个论坛: “密码学，标准与公共政策” held in Hotel Sofitel in Redwood City with 50 attendees: the “Conference” starts at 9:00 a.m. and ends at 3:00 p.m.这就是首届RSA会议!

● Bidzos1995年访问中国外经部和中国科学院信息安全国家重点实验室。

Jim Bidzos引领的RSA会议是美国信息革命的大本营，会议讨论密码技术革命将把Internet引向何方？ 给人民带来哪些福祉？显然，这个会议对美国NSA带来一系列麻烦！

“NSA Agents Threaten to Kill Bidzos of RSA?”~传言

U.S. government tried to mandate availability of all encryption keys via “key escrow” and/or “Clipper Chip” (1993)

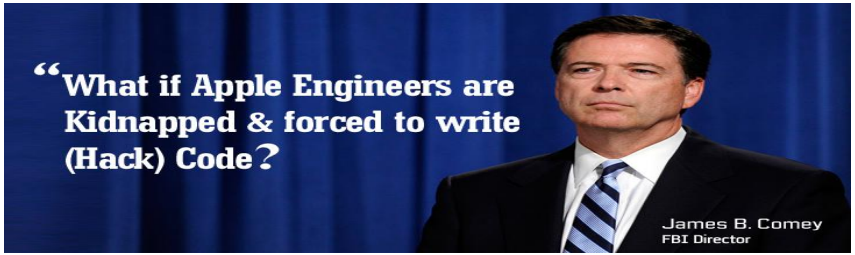
美国政府1993年颁布了EES标准（Escrow EncryptIon Standard)，目的是通过代理机构对用户密钥实行法定托管。如果监视机构向法院提供的证据表明，密码使用者是利用密码在进行危及国家安全和违反法律规定的事，经过法院许可，政府可以从托管代理机构取来密钥直接侦听通信。然而，美国民众利用信息自由法案，隐私法案强烈反对美国政府的做法，EES流产！（美国人称 “第一次密码战” .）

美国年青人所投入的史无前例的信息技术大革命,直接挑战了美国国家安全局NSA 对数据的处理能力。事实上：

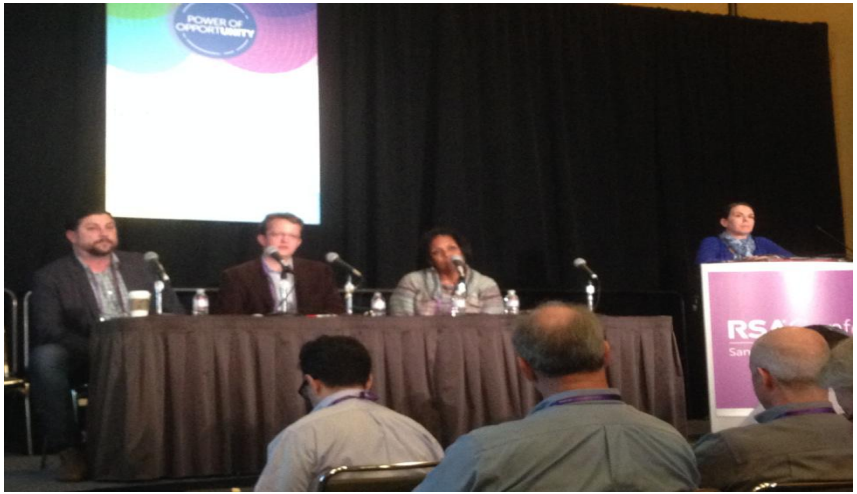
1. 70年代,NSA失去了对加密技术的垄断权； 2. 80年代通讯信号从模拟向数字转化。一个数据包所含的比特数据量猛增,很难从数据包里窃听到内容。 3.90年代信息超载,也就是海量数据现象，NSA已经很难处理窃听到的数据，于是所谓密钥托管的芯片问题提出来…. 4. 以往卫星通讯主宰全球的信息传递，现在的光纤将全球的各个站点包括卫星地面站都连接起来。

●1987年:中国发送首封电子邮件。1990年：中国顶级域名CN注册成功，中国的网络有了自己的身份标识。1994年：中国实现了Internet的全功能连接。从此，我国被国际上正式承认为“租用美国Internet的国家”。1995年8月8日，建在中国教育和科研计算机网上的水木清华BBS正式开通，成为中国大陆第一个联在美国Internet上的BBS。

今年RSA会议抛出一个研究问题:Encryption and Back Door: The Line Between Privacy and National Security



大家热烈地讨论：为了国家的安全---设置后门，弱化民间密码是否必要？



由人工智能引起的一场机器革命已经开始

The Second Machine Age

●美国白宫科技政策办公室于2016年10月发布了题为《为人工智能的未来做好准备》和《国家人工智能研发战略规划》两份重要报告。报告认为,人工智能技术对社会各领域的影响越来越深刻,教育是人工智能应用的一个重要领域。教育人工智能(Educational Artificial Intelligence）是人工智能与学习科学相结合的一个新领域,目前,

教育人工智能的关键技术主要体现在知识的表示方法、机器学习与深度学习、自然语言处理、智能代理、情感计算等方面,其应用与发展趋势集中在智能导师与助手、智能测评、学习伙伴、数据挖掘与学习分析等领域。基于此,

迫切需要在各级各类教育中强化人工智能方面的人才培养,以应对人工智能的快速发展。

● **Quantum computers pose a huge threat to security, and the NIST wants your help!**NIST请公众提出和测试“量子抵抗”加密方案如果大规模量子计算机被建立，他们将能够破译目前使用的许多公钥密码系统。一旦这种机器广泛可用,则将严重损害互联网中的数字通信的保密性和完整性。NIST在征求关于“新的公钥密码技术标准”的工作，方案提交截止日期是2017年11月30日。增加了研制会思维机器的迫切性!

结束