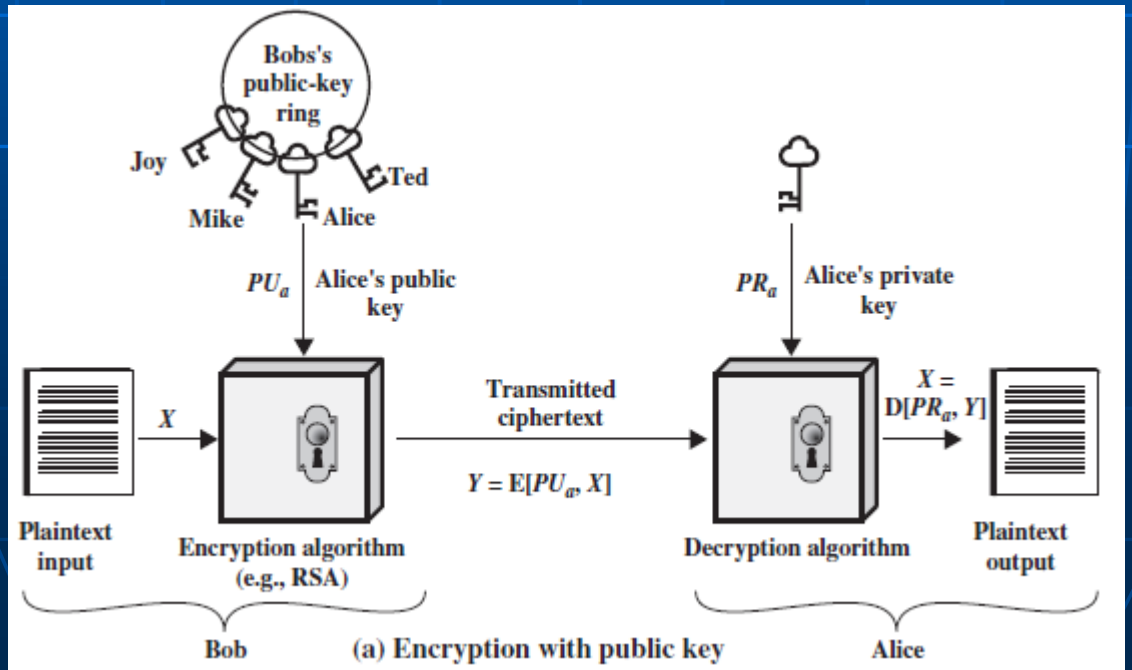
密码理论与技术

典型安全方案概览（续）

RSA和Goldwasser公钥加密方案实例



公钥加密方案(3)

- 实　例:
- OAEP/RSA方案(1993,基于计算Euler函数的问题难解)
- ElGamal方案(1985,基于判定性Diffie-Hellman问题难解)
- Cramer-Shoup方案(1999,判定性Diffie-Hellman问题难解)

等等

M.Bellare　*V.Shoup*　*P.Rogaway*　*El Gamal*

公钥加密方案(4A)

“记住，孩子们，不再使用的那些密码参数，在程序里必须清零哦”

- RSA方案(1978，参阅教程9.2)

- (1)公钥-私钥生成算法
- 生成大的素数p,q(p≠q)、计算整数N=pq、生成一个奇整数*e*和一个整数d，d、*e*和Euler函数φ(N)(=(p-1)(q-1))满足这样的关系：(e,φ(N))=1且$ed=1 \bmod \varphi(N)$ (注意：第一个条件保证第二个线性同余方程确实有解d)。
- RSA公钥pk=(N,e), RSA私钥sk=(*d*,*p*,*q*)。
- (2)加密算法E(pk,M)
- 对任何明文M: 1≦M≦N-1，生成密文$y = M^e \bmod N$。
- (3)解密算法D(sk,y)
- 对密文y，计算$M = y^d \bmod N$。

公钥加密方案(4B)

- RSA方案(续)

- (4)解密算法为什么正确

  对$y = M^e \bmod N$，若$(M, N)=1$则有

  $$y^d \bmod N = M^{ed} \bmod N = M^{1+k\varphi(N)} \bmod N$$

  $$= M\,(M^{\varphi(N)} \bmod N)^k \bmod N = M \bmod N = M。$$

- 若$(M, N)\neq 1$，解密结果也正确，详见后续的讨论。

- (5)RSA方案为什么安全：基本的依据

- 仅仅基于公开的信息e和N，不存在现实可行的算法A计算出$\varphi(N)$，

- 因此也无法推算出用以解密的私钥d。

公钥加密方案(5)

一个通用的方案构造(Goldwasser,1982)

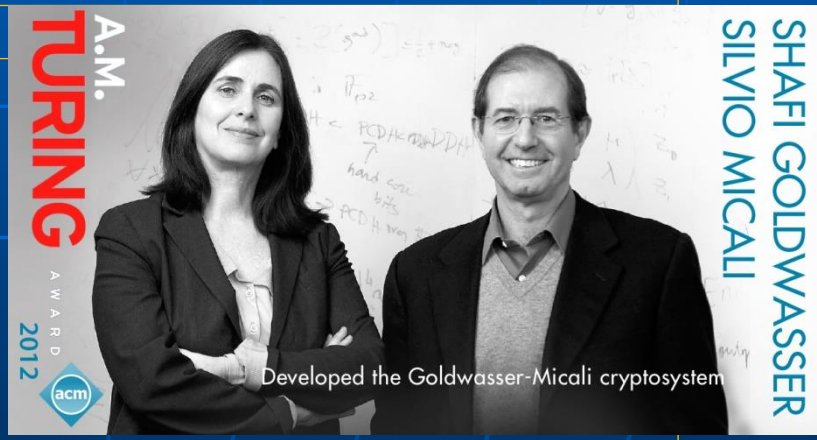
带陷门的单向函数f:

- $f(\alpha, x)$易计算;
- 计算 $f(\alpha, x)$的逆映像困难;
- 已知α的陷门β时， 计算 $f(\alpha, x)$的逆映像容易;

Goldwasser方 案

KG: 以α为公钥, β 为私钥

- 加密算法$E(\alpha, m)$:
  生成与m相同字长的随机数r;
  密文$y = f(\alpha, r)||(r \oplus m)$;
- 解密算法$D(\beta, y)$:
- 分离y的前缀u和后缀v;
- 计算$r = g(\beta, u)$，其中g是f的逆映像：$g(\beta, f(\alpha, x)) = x$;
- 计算$M = r \oplus v$。



对称及公钥加密方案小结(1)

	对称方案	公钥方案
1) 灵活性	密钥共享	无须共享任何秘密， 仅接收方持有秘密(私钥)。
2) 安全设计依据	组合密码函数	带陷门的单向函数
3) 效率	计算效率高， 适合于长明文流的加密(>1GB) 典型密钥长度~100bit	计算效率相对较低， 仅适合于短明文加密(~100KB) 典型密钥长度： 普通密码体制~1000bit 椭圆曲线密码体制~200bit

对称及公钥加密方案小结(2)

- 问题：如何有效利用两类方案的优点?
- 答案：混合加密

E.Fujisaki

- A　　pk公开　　B(sk)

明文M　　3.传递Z　　4.获取密钥：$K = D^*(sk, Z)$

1.生成对称密钥K(~100bit)

2. $Z=E^*(pk,K)$

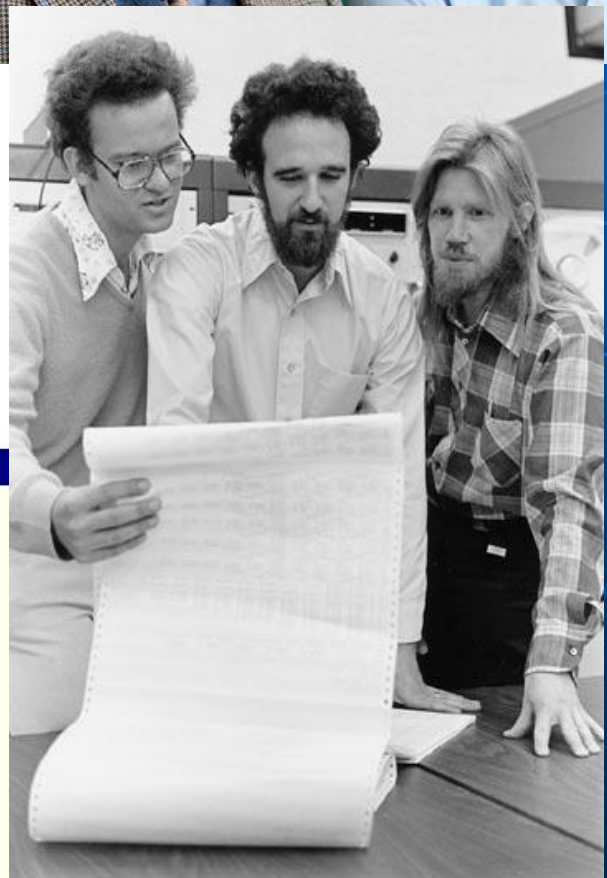
5. 加密(长)明文M：

$Y=E(K,M)$　　7.解密$M=D(K, Y)$

6.传递Y

T.Okamato & E.Fujisaki 混合加密之父

Diffi和Hellman，
2016年图灵奖获得者



SHAFI GOLDWASSER

1958 –

Israeli-American Computer Scientist

"Let's not try to define knowledge, but try to define zero-knowledge."

- Pioneer of modern cryptography: co-inventor of zero-knowledge proofs
- Professor at MIT and Weizmann Institute
- A.M. Turing Award 2012

  "Along with Silvio Micali, for transformative work that laid the complexity-theoretic foundations for the science of cryptography, and in the process pioneered new methods for efficient verification of mathematical proofs in complexity theory."

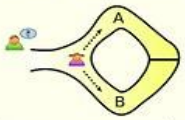
- Gödel Prize in theoretical computer science 1993 and 2001

Find out more about Shafi:

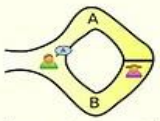
Watch Shafi explain the difference between mathematics and computer science (10 mins):

Zero-knowledge proofs

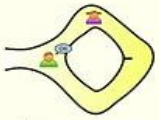
Prove that you know "something", without revealing "something."
Let's say Peggy knows the secret password for the door in Ali Baba's cave. She wants to convince Victor that she knows the password without telling him what the password is.



1) Peggy tosses a coin to decide on which path to enter the cave, A or B.



2) Victor shouts which path Peggy should take to exit the cave.



3) Peggy always appears at the right exit.

If Peggy doesn't know the password, and they do this 20 times, she only has a 1-in-a-million chance to always get the right exit!