Cryptography and Network Security

Lecture 00 – Cryptography

(Summary of the award-winning talk by Ron Rivest)

Ediz ŞAYKOL

Euclid

There are infinitely many primes:
2, 3, 5, 7, 11, 13, . . .

The greatest common divisor of two numbers is easily computed (using “Euclid’s Algorithm”):
$\gcd(12, 30) = 6$

Fermat and Euler

Fermat's Little Theorem (1640):
For any prime p and any a, $1 \leq a < p$:

$$a^{p-1} = 1 \pmod{p}$$

Euler's Theorem (1736):
If $\gcd(a, n) = 1$, then

$$a^{\phi(n)} = 1 \pmod{n},$$

where $\phi(n) = \#$ of $x < n$ such that $\gcd(x, n) = 1$.

C.F. Gauss

Published *Disquisitiones Aritmeticae* at age 21

"The problem of *distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors* is known to be one of the most important and useful in arithmetic. . . . the dignity of the science itself seems to require solution of a problem so elegant and so celebrated."

W.S. Jevons

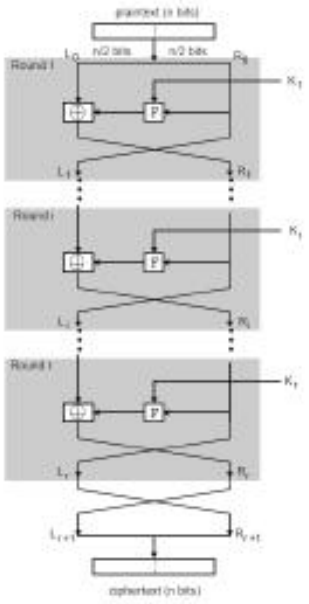
Published *The Principles of Science* (1874)

Gave world's first *factoring challenge*:

> *"What two numbers multiplied together will produce 8616460799 ? I think it unlikely that anyone but myself will ever know."*

Factored by Derrick Lehmer in 1903. ($89681 * 96079$)

US Data Encryption Standard (DES)



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.(?)

Public-Key Cryptography (Diffie-Helmann, November 1976)

- Each party A has a *public key* PK_A others can use to encrypt messages to A:

$$C = PK_A(M)$$

- Each party A also has a *secret key* SK_A for decrypting a received ciphertext C:

$$M = SK_A(C)$$

- It is easy to compute matching public/secret key pairs.
- Publishing PK_A does not compromise SK_A! It is *computationally infeasible* to obtain SK_A from PK_A. Each public key can thus be safely listed in a public directory with the owner's name.

Digital Signatures

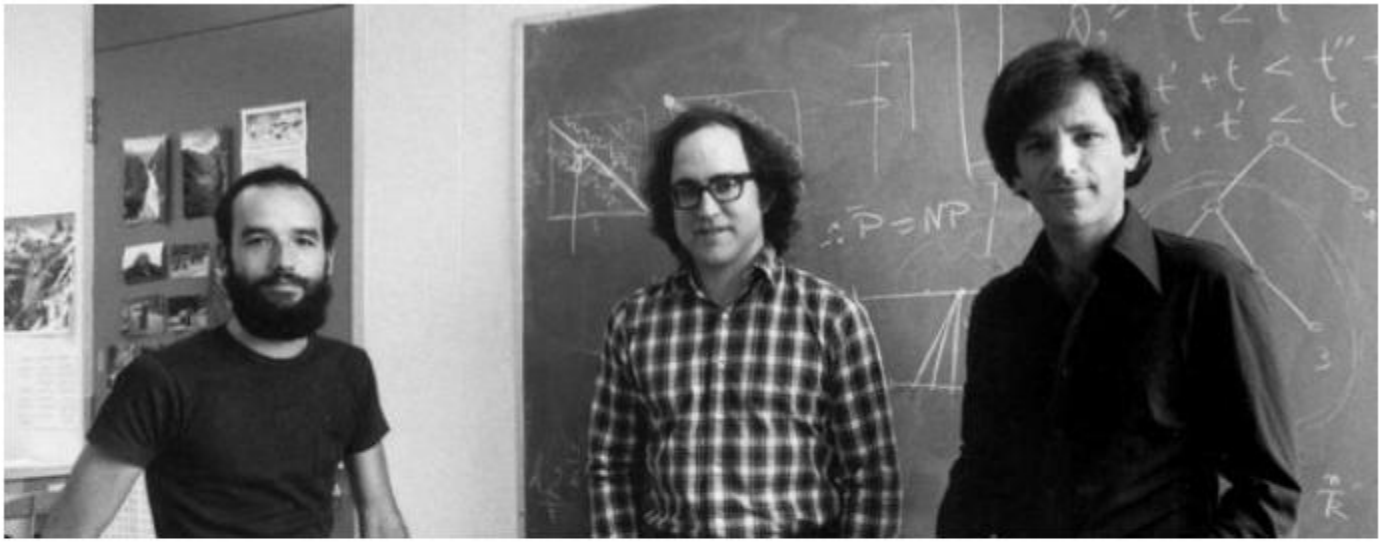
- Idea: sign with SK_A; verify signature with PK_A.
- A produces signature σ for message M

$$\sigma = SK_A(M)$$

- Given PK_A, M, and σ, anyone can verify validity of signature σ by checking:

$$M \stackrel{?}{=} PK_A(\sigma)$$

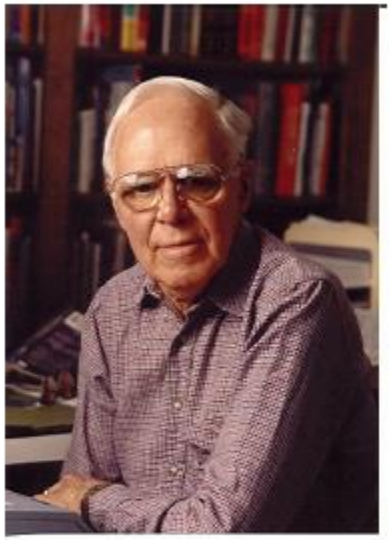
RSA (Rivest, Shamir, Adleman), 1977

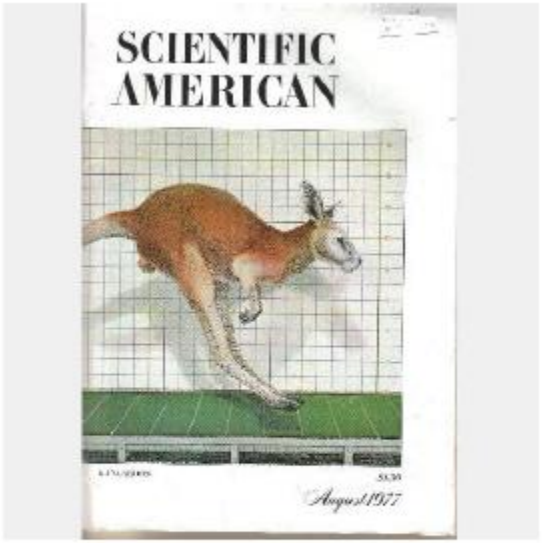


- Security relies (in part) on inability to factor product n of two large primes p, q.
- $PK = (n, e)$ where $n = pq$ and $\gcd(e, \phi(n)) = 1$
- $SK = d$ where $de = 1 \mod \phi(n)$
- Encryption/decryption (or signing/verify) are simple:

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

M. Gardner and RSA-129





- Described public-key and RSA cryptosystem in his Scientific American column, *Mathematical Games*
- Offered $100 to first person to break challenge ciphertext based on 129-digit product of primes. (Our) estimated time to solution: 40 quadrillion years

RSA-129 Factorization

- RSA-129 =

  ```
  114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541
  ```

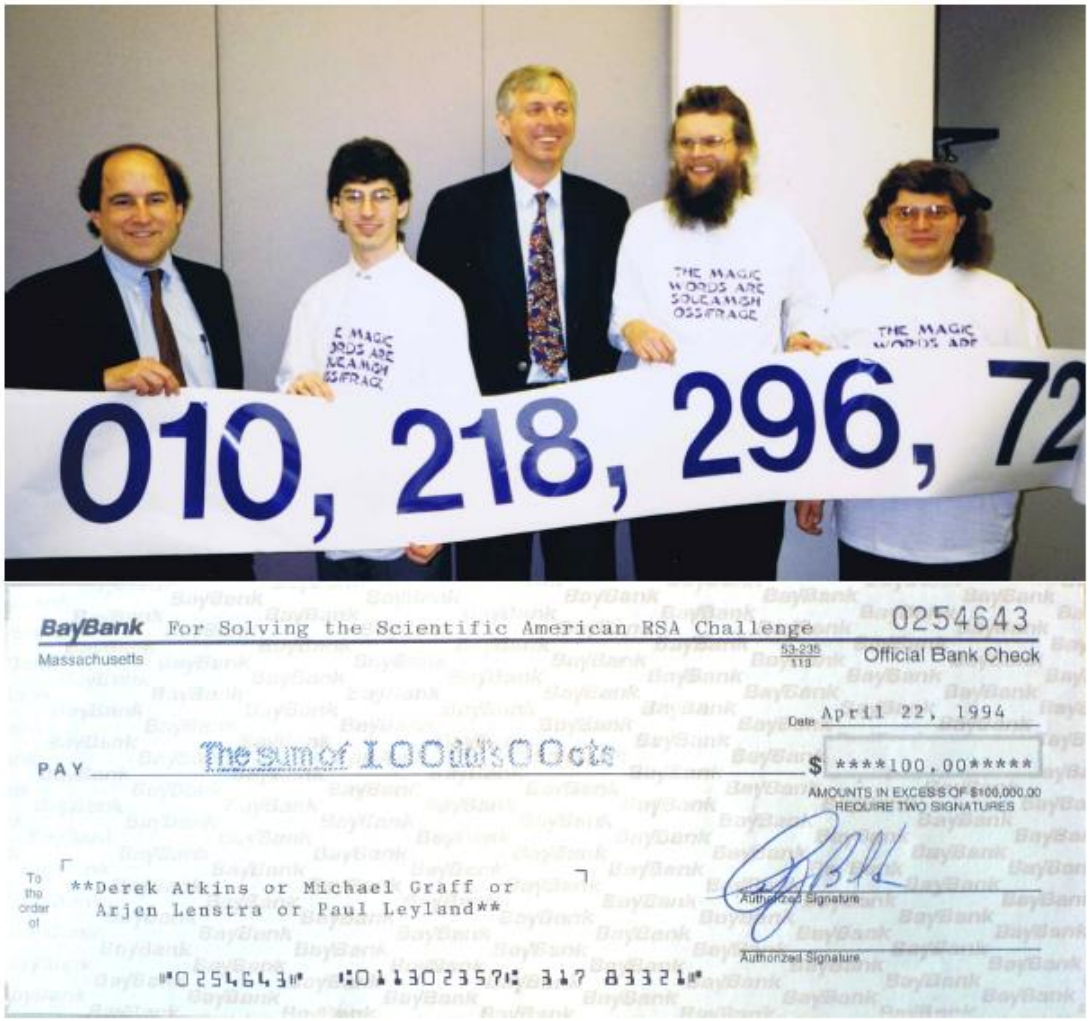
- Derek Atkins, Michael Graff, Arjen Lenstra, Paul Leyland: RSA-129 =

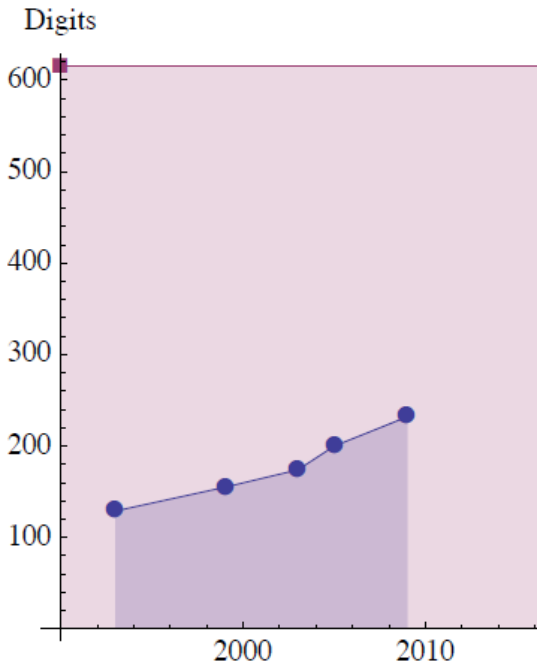
  ```
  3490529510847650949147849619903898133417764638493387843990820577 x 327691329932667095499619881908344614131776429679929425397982885 33
  ```

- 8 months work by about 600 volunteers from more than 20 countries; 5000 MIPS-years.
- secret message:

  The Magic Words Are Squeamish Ossifrage

April 1994

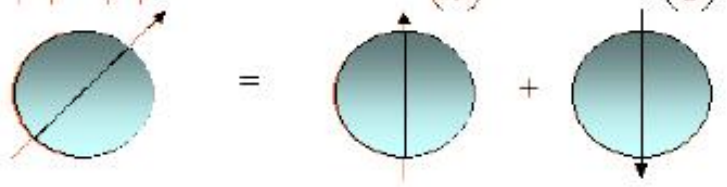

010, 218, 296, 72
BayBank
Massachusetts
For Solving the Scientific American RSA Challenge
0254643
53-235
113
Official Bank Check
Date April 22, 1994
PAY The sum of 100 dollars 00 cts
$ ****100.00*****
AMOUNTS IN EXCESS OF $100,000.00
REQUIRE TWO SIGNATURES
To the order of
**Derek Atkins or Michael Graff or
Arjen Lenstra or Paul Leyland**
Authorized Signature
Authorized Signature
"0254643" :011302357": 317 83321"


Digits
600
500
400
300
200
100
2000
2010

Quantum Computer (?)

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$
$$|\alpha|^2 + |\beta|^2 = 1$$

$$\alpha|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \beta|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$



In 1994, Peter Shor invented a fast factorization algorithm that runs on a (hypothetical) *quantum computer* and works by determining multiplicative period of elements mod n.

- In 2001, researchers at IBM used this algorithm on a (real) quantum computer to factor $15 = 3 \times 5$.

Homomorphic Encryption

- In 1978, Rivest, Adleman, and Dertouzos asked,

  "Can one compute on encrypted data, while keeping it encrypted?"

- In 2009, Craig Gentry (Stanford,IBM) gave solution based on use of lattices. If efficiency can be greatly improved, could be huge implications (e.g. for cloud computing).

Summary

- Cryptography is not the solution to all of our cybersecurity problems, but it is an essential component of any solution.
- Research in cryptography is a fascinating blend of mathematics, statistics, theoretical computer science, electrical engineering, and psychology.