

# The Evolution of Public Key Cryptography

Martin E. Hellman  
Stanford University

# Revolutionary or Evolutionary?

Revolutionary: Auguste Kerchoffs 1883  
The general system must be considered  
public information. Security resides solely  
in the secrecy of the key.

How can you have a public key?

# Evolutionary

Half the concept (privacy) occurred independently to three different groups almost simultaneously. In addition to Whit Diffie and me:

Ralph Merkle at UC Berkeley.

James Ellis, Clifford Cocks, and Malcolm Williamson at GCHQ.

# Diffie-Hellman AND Merkle



Photo by Chuck Painter  
© Stanford News Service

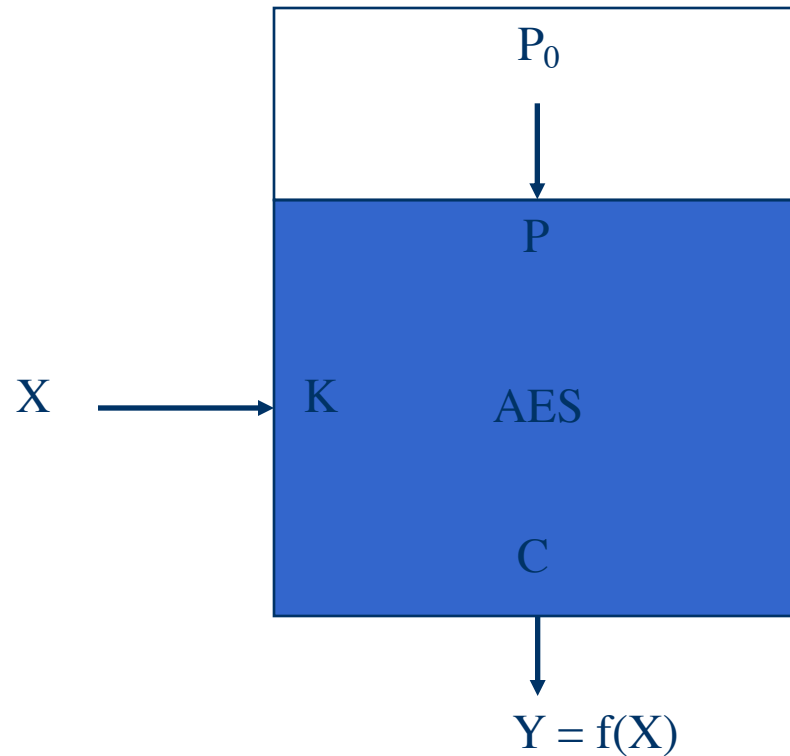
# Evolution via Cryptographic Hierarchy

See “New Directions in Cryptography”

1. One-Way Function
2. Conventional (Symmetric) Cryptosystem
3. Trap Door Cryptosystem
4. Public Key (Asymmetric) Cryptosystem

# One-Way Function

One-way functions are simpler than (conventional) cryptosystems.



# Trap Doors

While trap doors are associated with public key cryptography, they are fundamental to all cryptographic entities

Trap door quiz problem:  
Given  $Y=f(X)$  and  $Y$  find  $X$ .

Related to  $P =? NP$  question.

# Trap Door Cryptosystem

Information known only to the designer allows him to easily break the system.

This is the dream of every nation's military ... and their equivalent of NSA.

Trap door cryptosystems allow public key exchange.



# Public Key Cryptography

Whit Diffie and I developed the concept of a public key cryptosystem.

Ralph Merkle independently developed the concept of a public key distribution system and had a proof of concept.

“Diffie-Hellman” is a Merkle PKD system!

# Merkle's PKD Proposal

C.S. 244  
FALL 1974

Project 2 looks more reasonable, maybe  
because your description of Project 1 is muddled  
terribly. Talk to me about these today.  
Ralph Merkle

## Project Proposal

**Topic:** Establishing secure communications between separate  
secure sites over insecure communication lines.

**Assumptions:** No prior arrangements have been made between the two  
sites, and it is assumed that any information known  
at either site is known to the enemy. The sites,  
however, are now secure, and any new information will  
not be divulged.

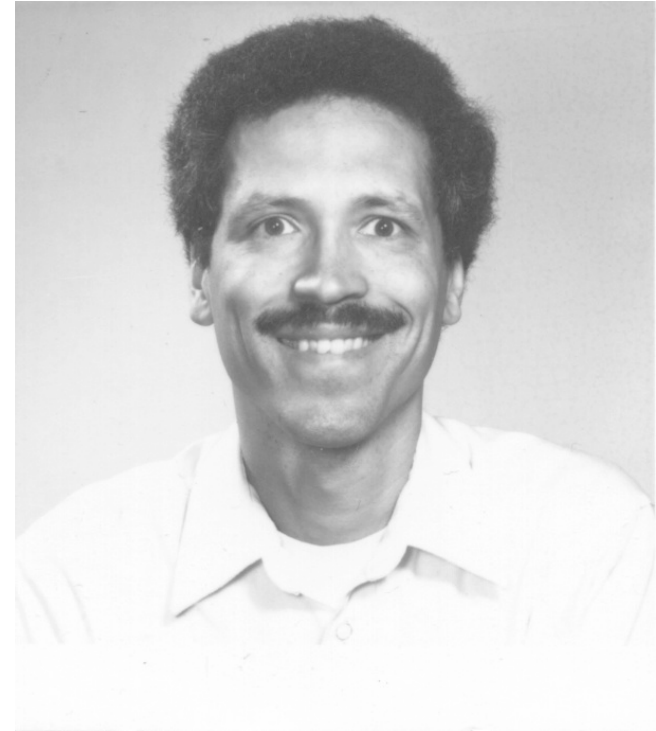
# CACM Rejected Merkle Paper

Editor: “[I] was particularly bothered by the fact that there are no references to the literature. Has anyone else ever investigated this approach?”

An Experienced Cryptography Expert: “the paper is not in the mainstream of present cryptography thinking ... I would not recommend that it be published.”

# John Gill, Unsung Hero #2


- Start with the simplest crypto-entity, a one-way function.
- John Gill suggested indices (discrete logs).
- $Y = \alpha^X \bmod q$  is fast:  
 $\alpha^9 = (\alpha^2)^2 \times \alpha$
- $X = \log_{\alpha}(Y)$  is slow



John Gill in 1976

# “Derivation” of Pohlig-Hellman Conventional Cryptosystem

- $\alpha, X \rightarrow Y$  easy (exponentiation)
- $\alpha, Y \rightarrow X$  **hard** (discrete log)
- $X, Y \rightarrow \alpha$  easy
  
- $P, K \rightarrow C$  easy (encipher)
- $C, K \rightarrow P$  easy (decipher)
- $P, C \rightarrow K$  **hard** (cryptanalysis)



X must be K!  
The key is in  
the exponent.

# Pohlig-Hellman Cryptosystem

$$C = P^K \text{ mod } q$$

$$P = C^D = P^{KD} \text{ mod } q$$

$$KD = 1 \text{ mod } \phi(q) = q-1$$



# RSA Public Key Cryptosystem

$$C = P^E \text{ mod } n$$

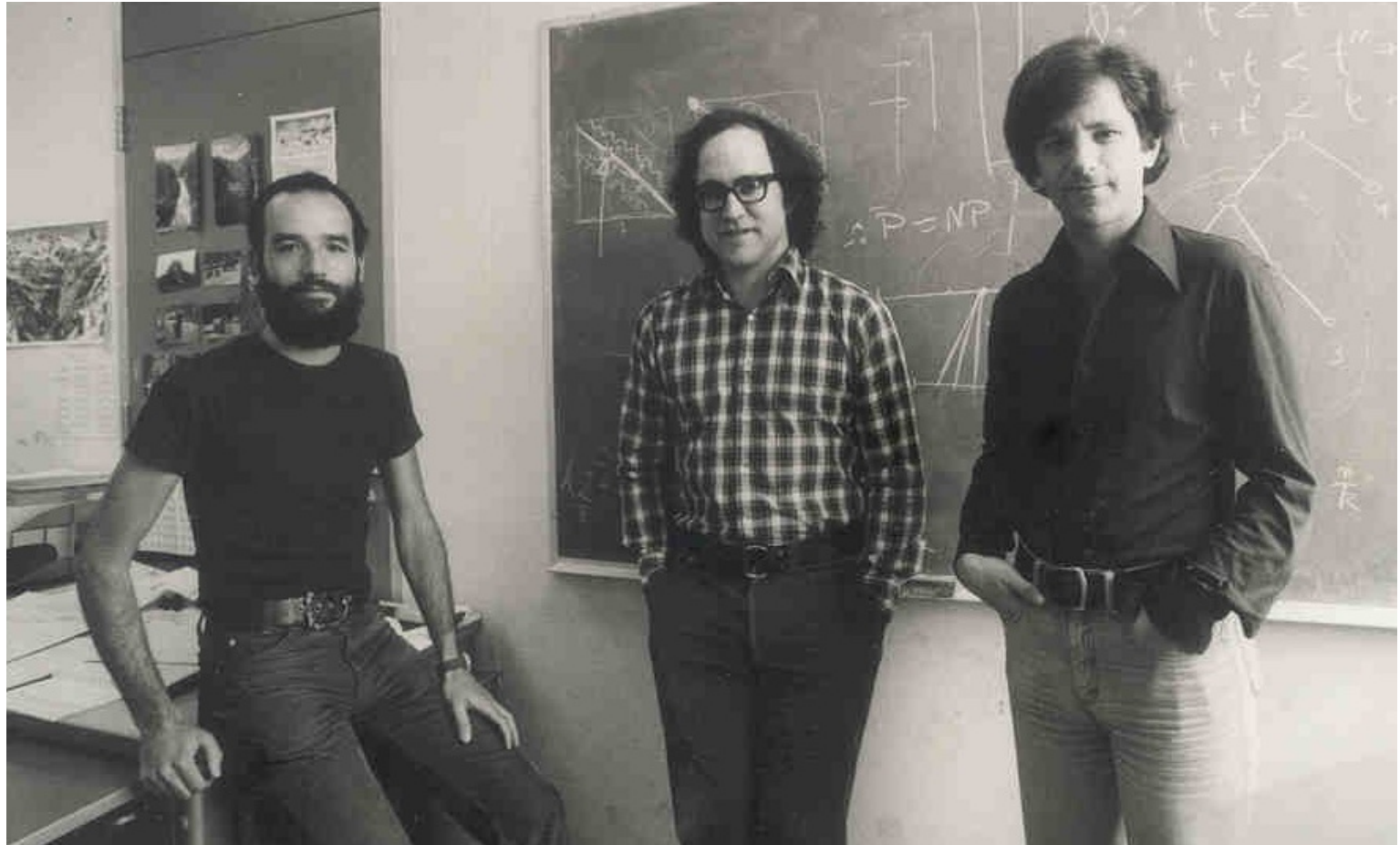
$$D = C^D = P^{ED} \text{ mod } n$$

$$ED = 1 \text{ mod } \phi(n) = (p-1)(q-1)$$

“Only” differences: K is called E, and q is replaced by  $n=pq$ .

P-H paper appeared a few months after RSA, but was submitted about a year before it. We totally missed that it could become a PKC.

# Rivest, Shamir & Adleman





# Diffie-Hellman-Merkle PKD

$$Y(i) = \alpha^{X(i)} \text{ mod } q$$

$$\begin{aligned} K(i,j) &= \alpha^{X(i)X(j)} \text{ mod } q \\ &= Y(i)^{X(j)} = Y(j)^{X(i)} \text{ mod } q \end{aligned}$$

I was trying to find a public key cryptosystem based on discrete logs when I came up with this public key distribution system instead.

Late one night in May 1976 I played with

$$Y = \alpha^X \text{ mod } q$$

Let  $\alpha$  and  $q$  be public (many variations).

Computing  $Y$  from  $X$  is easy (exponentiation).

Computing  $X$  from  $Y$  is hard (discrete log).

So try  $X(i) = i$ 's secret key and  $Y(i) =$  public key.

Then what? Eventually I tried:

$$Y(i)^{X(j)} = Y(j)^{X(i)} = \alpha^{X(i)X(j)} = K_{ij} \text{ mod } q$$

# Schroeppel: Unsung Hero #4

RSA originally used 256-bit keys, but Richard Schroeppel's work caused them to recommend  $\geq 200$  digits in their famous *CACM* paper.

Pomerance's Quadratic Sieve Method is related and he credits Schroeppel's unpublished work as the "inspiration" for the Quadratic Sieve.

# Kohnfelder: Unsung Hero #5

Loren Kohnfelder developed the concept of digital certificates in his 1978 MIT BS thesis under Len Adleman.

This created the foundation for VeriSign and all other Certificate Authorities (CA's).

# Born Classified?

March 1975: 56-bit key DES announced

$2^{56} = 10^{17}$  possible keys

$10^6$  keys/sec/chip

$10^6$  chips

$10^5$  seconds = 1 day

\$10,000/solution & decreasing an order of magnitude every 5 years. Short cuts?

## Technical or political problem?

January 1976: “Continuing will cause grave harm to national security.”

The “devil on my shoulder.” See my Turing Lecture write-up in the DEC 2017 issue of the *CACM*.

May 1976: PKC increased NSA’s concern

July 1977 J. A. Meyer letter to IEEE

October 1977: IEEE ISIT at Cornell

## **Resolution Begins**

1978: Call from Adm. Inman's office

“It's nice to see you don't have horns.”

“I am meeting with you against the advice of all the other senior NSA people. But I don't see any harm in talking.”

Adm. Inman signed a statement of support for my effort to assess and reduce the risk of nuclear deterrence.

It's better to have friends than enemies!

## **Resolution Grows**

1993 Congress requests NRC study

Cryptography's Role in Securing the Information Society (1996 CRISIS report)

All constituencies were represented, yet unanimous conclusions:

Relaxation of export restrictions

Classified information largely irrelevant

Key escrow not well defined. (Now too!)



This talk has been about the evolution of PKC, but also shows personal evolution.

I am a very different person from the 30-year old who battled NSA 40 years ago.

“Get curious, not furious”

**Friends are better than enemies.**