The Evolution of Public Key Cryptography
Martin E. Hellman
Crypto ’99
Santa Barbara, CA
August 18, 1999

ADD: Loren Kohnfelder and certificates

5min: ND 11/76: “We stand today on the brink of a revolution in cryptography.” While Whit and I had written that sentence before PKC had become a reality, clearly it has been part of the revolution in cryptography. But, as with any revolution, there was also an evolution that led to the revolution. That evolutionary process is easier to see in hindsight, and that will be the subject of my talk today. I will also try to give credit to some individuals whose work is often overlooked, but whose contributions were clearer to those of us working in the early days of the field.

In ND, we noted one aspect of the evolution: the trend toward decreasing secrecy in cryptographic systems. This was first clearly enunciated by Kerchoffs in 1881, when he distinguished between the general system - which must be assumed to be known to one’s opponents - and the secret key. Prior to that time (and unfortunately even today), systems were proposed that were unbreakable “if only we can keep the design of the cipher secret from our opponents.”

15:20 min ***John Gill*** and indices: one-way -> conventional -> PKD + PKC.

Show key pages and equations.

Pohlig-Hellman appeared 1/78 and had been submitted 6/76.

RSA appeared 2/78 but had been submitted about a year after P-H and preprints had been sent to key researchers in the area.

10:30 min Trap doors. PKC’s sometimes even called “trap door cryptography.” But trap doors (as noted in ND) are more basic.

1-way fnctn => trap door quiz problem

DES (and earlier somewhat) made us wonder about trap door cryptosystems, which (as shown in ND) allow the construction of a PKD system.

5:35 min ***Merkle’s*** puzzle PKD. Initially independent interest in PK, later moved to Stanford and worked with my group. PK was in the air! or did a muse whisper in our ears? Merkle deserves equal credit with D&H for the PK invention.

10:45 min   Evolution of Factoring (clearly related to evolution of PKC) and Discrete Logs: the work of ***Richard Schroeppel***.

Morrison-Brillhart’s CF method factored F7 in 1970, but did not analyze run time.

Schroeppel analyzed showing the now familiar subexponential behavior and circulated result. Knuth referenced it (vol 2, 2nd ed, 1981) and repeated key parts (with errors tho!)

Rich also came up with an improvement which allowed sieving and which he predicted would cut exponent by factor of two and allow factorization of F8 in about one year. While working on F8 1975-76, he was beat by Richard Brent using Pollard's rho method - usually much slower, but worked here due to highly unequal size of factors.

Show Rich's approach.

Quadratic sieve (1984) clearly builds on Schroeppel's work (1975 but …) .

5:50 min GCHQ paper? Parallel universe idea.

5:55 min One last aspect of the evolution of PKC: DeVoe Terrace. The wisdom of foolishness.

$$Y = \alpha X \% q$$

$X \rightarrow Y$ is one-way, with α and q known. But α and/or q could be inputs.

Key musings to find Pohlig-Hellman conventional cryptosystem (q public):

$\alpha, X \rightarrow Y$	easy	(exponentiation)
$X, Y \rightarrow \alpha$	easy	($\alpha = Y\ 1/X \% q-1 \ \% q$)
$\alpha, Y \rightarrow X$	hard	(discrete log)

$P, K \rightarrow C$	easy	(enciphering)
$C, K \rightarrow P$	easy	(deciphering)
$P, C \rightarrow K$	hard	(cryptanalysis)

$C = PK \% q$ $\qquad$ $P = C1/K \% q-1 \% q$

RSA: $C = PE \% n$ $\qquad$ $P = C1/E \% \phi(n) \% n$

Key musings to find Diffie-Hellman key exchange protocol (α and q public):

If Y is the public key, X could be the secret key.

How can A compute (XA,YB) → K?

K = XA * YB = XA *αX_B not useful.

K = XA ^ YB = XA ^ αX_B not useful.

K = YB ^ XA = [αX_B] X_A = α X_A X_B !!!

Schroeppel’s Factoring Algorithm

If $x2 = y2 \% n$ then

$(x+y)(x-y) = kn = kpq$ so

$GCD(x+y, n) \in \{1, p, q, n\}$

CF: $x/b \approx m = [\sqrt{n}]$ and (surprisingly)

$length(x2 \% n) = length(n)/2$ so it can factor numbers twice as long.

The most time consuming step is trial division of $x2 \% n$ by the set of “small” primes to see if $x2 \% n$ is “smooth.”

Schroeppel’s idea: sieving to double the length of numbers which can be factored:

$$(m+A)(m+B) - n = (m2-n)+ m(A+B) + AB$$
$$= O(\sqrt{n}) + O(\sqrt{n}) \quad + O(1)$$

$$(m+A+3)(m+B) - n$$
$$= [(m+A)(m+B) - n] + 3(m+B)$$

eliminates need for trial division (sieve!)

The $\{m+A\}$ are treated as additional primes.