Diffie-Hellman - Key Exchange (Discrete Log Problem)

Ron Rivest - new faculty member MIT (1975)

read paper.

ONE WAY FUNCTION -> easy forwards
hard inverses

Convinced Adi Shamir, Leonard Adleman

GOAL: Public Key Cryptosystem (asymmetric)

Rivest had Ideas
Shamir had Ideas
Adleman shot them down.

Marc Denon - Year

Passover Party 1977 (Mar-stor)

Overnight -> stretched out RSA encryption

Patent -> Company -> Sold
Alice wants people to be able to send secure msg to her.

Alice generates 2 private keys: \( p, q \) large primes.

Calculate \( n = pq \), \( n \) will public key.

(\text{security is based on factoring being hard})

Calculate \( \phi(n) = (p-1)(q-1) \) \( \equiv \) Private

Alice pick a random \( e \), \( \gcd(e, \phi(n)) = 1 \)

\( e \) is another Public key.

Alice computes \( d = e^{-1} \mod \phi(n) \) via EEA.

\( d \) is another private key.

Public: \( n, e \)

Private: \( p, q, d, (\phi(n)) \)

Send to Alice: Pick \( M \) \( 0 < M < n \)

Bob computes \( C = M^e \mod n \)

sends \( C \) to Alice.

Alice receives \( C \). Computes \( C^d \equiv M \mod n \)

\( C^d = (M^e)^d = M^{ed} = M^{k\phi(n)+1} \equiv (M^\phi(n))^k \cdot M \equiv 1 \cdot M \mod n \)
\( n = 11 \times 17 = 187 \)
\( \phi(n) = 10 \times 16 = 160 = 2^4 \times 2 \times 5 = 2^5 \times 5^1 \)

\( e = 21 \) what is \( d \)?

\( d = 21^{-1} \mod 160 \)

\[
\begin{align*}
160 &= 7 \times 21 + 13 \\
21 &= 13 + 8 \\
13 &= 8 + 5 \\
8 &= 5 + 3 \\
5 &= 3 + 2 \\
3 &= 2 + 1 \\
\end{align*}
\]

\[
\begin{align*}
3 - 2 &= 1 \\
3 - (5 - 3) &= 1 \\
2 \times 3 - 1 \times 5 &= 1 \\
2(8 - 5) - 1 \times 5 &= 1 \\
2 \times 8 - 3 \times 5 &= 1 \\
2 \times 8 - (13 - 8) &= 1 \\
5 \times 6 - 3 \times 13 &= 1 \\
5 \times (21 - 13) - 3 \times 13 &= 1 \\
5 \times 21 - 8 \times 13 &= 1 \\
5 \times 21 - 8 \times 160 + 56 \times 21 &= 1 \\
61 \times 21 - 8 \times 160 &= 1 \\
\end{align*}
\]

\( d = 61 \)

\( M = 9 \times 7 \)
\( C = 97^{21} \equiv 20 \mod 187 \)
\( M = 20^{61} \equiv 97 \mod 187 \)

Alice computes

Opponent sees \( n = 187, \ e = 21 \) they have difficulty computing \( d \).

If \( \text{factor, then } \Rightarrow \phi(n) \Rightarrow d \).
(b) Now knowing $\phi(n)$ can help you break it.

Code how to convert text/bits $\geq M$

\[
\begin{align*}
    n &= 187 = p^2 \\
    \phi(n) &= 160 = (p-1)(q-1) \\
    &= pq - p - q + 1
\end{align*}
\]

\[
\begin{align*}
    n - \phi(n) &= 27 = p + q - 1 \\
    28 &= p + q \\
    q &= (28 - p)
\end{align*}
\]

\[
\begin{align*}
    187 &= p(28 - p) \\
    187 &= 28p - p^2 \\
    p^2 - 28p + 187 &= 0
\end{align*}
\]

Quadratic formula will work with large \( n \) inputs

\[
\begin{align*}
    C^{A - 1} \mod n &= 2 \times 26^2 + 0 \times 26^1 \times 19 \times 26^0 \\
    \text{HomE} &= 7 \times 26^3 + 14 \times 26^2 + 12 \times 26^1 + 4 \times 26^0
\end{align*}
\]