The RSA Algorithm

Security of the RSA algorithm

- **Brute force:** This involves trying all possible private keys.
- **Mathematical attacks:** There are several approaches, all equivalent in effect to factoring the the product of two primes (Integer Factorization Problem (IFP)).
  Given a composite integer n of the form $n = p \times q$, to find the prime factors p and q.
  IFP is computationally infeasible (not solvable in polynomial-time factoring algorithm when n is very large, for example, when n is 1024 bits or 2048 bits number.
- **Timing attacks:** These depend on the running time of the decryption algorithm.

The RSA Algorithm

Problem:

The ciphertext message produced by the RSA algorithm with the public key $(e, n) = (223, 1643)$ is:
1451 0103 1263 0560 0127 0897.
Determine the original plaintext message.
Use the standard encoding procedure:
A = 01, B = 02, . . ., Z = 26,
, = 27, . = 28, ? = 29,
0 = 30, 1 = 31, . . ., 9 = 39, ! = 40,
with 00 as the blank space.

The RSA Algorithm

Solution:

- Here $e = 223$, $n = 1643 = 31 \times 53 = p \times q$, say, where p and q are distinct primes.
- $\phi(n) = \phi(1643) = (p-1) \times (q-1) = 30 \times 52 = 1560$.
- Using the Extended Euclid's GCD algorithm, $ed \equiv 1 \pmod{\phi(n)}$, that is, $d = 7$.
- The private key is then $(d, n) = (7, 1643)$.
- The given ciphertext blocks are as follows:
  $C_1 = 1451$,
  $C_2 = 0103$,
  $C_3 = 1263$,
  $C_4 = 0560$,
  $C_5 = 0127$
  $C_6 = 0897$.

The RSA Algorithm

Solution (Continued...):

- The deciphertext (recovered plaintext) of each block C_i is given below (using the repeated square-and-multiply method).
- $M_1 = C_1^d \pmod{n} = 1451^7 \pmod{1643} = 180$
- $M_2 = C_2^d \pmod{n} = 103^7 \pmod{1643} = 516$
- $M_3 = C_3^d \pmod{n} = 1263^7 \pmod{1643} = 122$
- $M_4 = C_4^d \pmod{n} = 560^7 \pmod{1643} = 500$
- $M_5 = C_5^d \pmod{n} = 127^7 \pmod{1643} = 141$
- $M_6 = C_6^d \pmod{n} = 897^7 \pmod{1643} = 523$
- Hence, the original plaintext message using the decoding method given here is as follows:
  $M = M_1 M_2 M_3 M_4 M_5 M_6 = 18\ 05\ 16\ 12\ 25\ 00\ 14\ 15\ 23$
  $= \text{REPLY NOW}$

The RSA Algorithm

Online Demo on RSA Algorithm

- Generating private/public keys pair
- Encrypting a message
- Decrypting a message

https://8gwifi.org/rsafunctions.jsp

https://www.mobilefish.com/services/rsa_key_generation/rsa_key_generation.php

Diffie-Hellman Key Exchange Protocol

Overview

- Diffie-Hellman key agreement (also called exponential key exchange or Diffie-Hellman key exchange) provided the first practical solution to the secret key distribution problem.
- It is based on public-key cryptography.
- This protocol enables two parties, say A and B, which have never communicated before, to establish a mutual secret key by exchanging messages over a public channel.

Inventors

Figure: Prof. Whitfield Diffie

Inventors

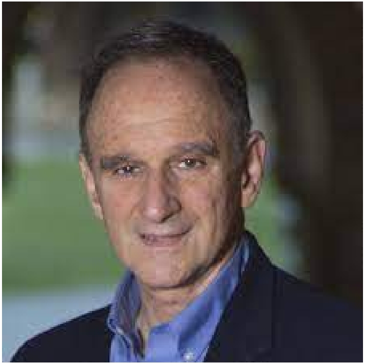

Figure: Prof. Martin Hellman

Me with Prof. Martin Hellman (15 February 2018 at IIIT Hyderabad)

Diffie-Hellman Key Exchange Protocol (continued...)

Global Public Elements

- q : a sufficiently large prime, such that it is intractible to compute the discrete logarithms in $Z_q^* = \{1, 2, \cdots, q-1\}$
(Given α, q and $y = \alpha^x \pmod q$), to find discrete logarithm $x \in Z_q^*$).
- α : $\alpha < q$ and α a primitive root of q.
(Compute $\alpha^1 \pmod q$, $\alpha^2 \pmod q$, $\cdots$, $\alpha^{q-1} \pmod q$.
If all are distinct and $\alpha^{q-1} \pmod q = 1$, α is primitive root of q)

User A Key Generation

- Select private X_A such that $X_A < q$
- Calculate public Y_A such that $Y_A = \alpha^{X_A} \mod q$

$A \rightarrow B : \{Y_A, q, \alpha\}$
Here $A \rightarrow B : M$ denotes party A sends a message M to party B.

Diffie-Hellman Key Exchange Protocol (continued...)

User B Key Generation

- Select private X_B such that $X_B < q$
- Calculate public Y_B such that $Y_B = \alpha^{X_B} \mod q$

$B \rightarrow A : \{Y_B\}$

Generation of secret key by User A

- $K_{A,B} = (Y_B)^{X_A} \mod q$

Generation of secret key by User B

- $K_{B,A} = (Y_A)^{X_B} \mod q$

Diffie-Hellman Key Exchange Protocol (continued...)

Summary

User A	User B
1. Select private X_A	
2. Calculate public Y_A	
3. $\xrightarrow{Y_A = \alpha^{X_A} \mod q}$	
	1. Select private X_B
	2. Calculate public Y_B
	3. $\xleftarrow{Y_B = \alpha^{X_B} \mod q}$
4. $K_{A,B} = (Y_B)^{X_A} \mod q$	4. $K_{B,A} = (Y_A)^{X_B} \mod q$

Correctness Proof

$$\begin{aligned}
K_{A,B} &= (Y_B)^{X_A} \mod q \text{ [User A]} \\
&= (\alpha^{X_B} \mod q)^{X_A} \mod q \\
&= (\alpha)^{X_B \cdot X_A} \mod q \\
&= (\alpha^{X_A})^{X_B} \mod q \\
&= (\alpha^{X_A} \mod q)^{X_B} \mod q \\
&= (Y_A)^{X_B} \mod q \\
&= K_{B,A} \text{ [User B]}
\end{aligned}$$

Problem [Diffie-Hellman Key Exchange]

Users A and B use the Diffie-Hellman key exchange technique with a common prime $q = 71$ and a primitive root $\alpha = 7$.
(a) If user A has private key $X_A = 5$, what is the A's public key Y_A?
(b) If user B has private key $X_B = 12$, what is the B's public key Y_B?
(c) What is the secret shared key?

Solution: Here $q = 71$ and $\alpha = 7$.
(a) A's public key Y_A is given by

$$\begin{aligned} Y_A &= \alpha^{X_A} \bmod q \\ &= 7^5 \bmod 71 \\ &= (7^1 \bmod 71) \times (7^4 \bmod 71) \bmod 71 \\ &= 51 \end{aligned}$$

Diffie-Hellman Key Exchange Protocol (continued...)

Problem [Diffie-Hellman Key Exchange] (Continued...)

(b) B's public key Y_B is given by

$$\begin{aligned} Y_B &= \alpha^{X_B} \bmod q \\ &= 7^{12} \bmod 71 \\ &= (7^4 \bmod 71) \times (7^8 \bmod 71) \bmod 71 \\ &= 4 \end{aligned}$$

(c) The secret shared key K is given by

$$\begin{aligned} K_{A,B} &= (Y_B)^{X_A} \bmod q \text{ [User A]} \\ &= 4^5 \bmod 71 \\ &= 30 \end{aligned}$$

Problem [Diffie-Hellman Key Exchange] (Continued...)

$$\begin{aligned} K_{B,A} &= (Y_A)^{X_B} \mod q \text{ [User B]} \\ &= 51^{12} \mod 71 \\ &= 30 \end{aligned}$$

$K = K_{A,B} = K_{B,A} = 30$ is the required secret shared key between A and B.

■

Diffie-Hellman Key Exchange Protocol (continued...)

Online Demo on Diffie-Hellman Key Exchange Protocol

- Generating primitive root of prime
- Computing the shared session key between two parties

`http://www.irongeek.com/diffie-hellman.php?`

Further Readings (Cryptography and Network Security)

- William Stallings, “Cryptography and Network Security: Principles and Practices”, Pearson Education, 2010.
- Behrouz A. Forouzan, “Cryptography and Network Security”, Special Indian Edition.
- Bernard Menezes, “Network Security and Cryptography”, Cengage Learning, 2010.
- A. Menezes, P. Oorschot and S. Vanstone, “Handbook of Applied Cryptography”, CRC Press.
- B. Schneier, “Applied Cryptography”, Reading, MA: Addison-Wesley, 2006.
- D. Stinson, “Cryptography: Theory and Practice”, Chapman & Hall/CRC, 2006.
- Neal Koblitz, “A course in number theory and cryptography”, Springer.

Thank you