Diffie Hellman Key Exchange

LIKE
COMMENT
SHARE
SUBSCRIBE

What is primitive root of a number?

$5 \Rightarrow 2$

The primitive root of a prime number n is an integer r between[1, n-1] such that the values of r^x(mod n) where x is in the range[0, n-2] are different.

EXAMPLE

2 is a primitive root mod 5, because for every number a relatively prime to 5, there is an integer z such that $2^z \equiv a$.
All the numbers relatively prime to 5 are 1, 2, 3, 4, and each of these (mod 5) is itself $\big($for instance 2 (mod 5) = 2$\big)$:

- $2^0 = 1, \ 1 \pmod 5 = 1$, so $2^0 \equiv 1$
- $2^1 = 2, \ 2 \pmod 5 = 2$, so $2^1 \equiv 2$
- $2^3 = 8, \ 8 \pmod 5 = 3$, so $2^3 \equiv 3$
- $2^2 = 4, \ 4 \pmod 5 = 4$, so $2^2 \equiv 4$.

For every integer relatively prime to 5, there is a power of 2 that is congruent.

Primitive Root of 11 is 7.

```
(7^1)mod 11= 7
(7^2)mod 11= 5
(7^3)mod 11= 2
(7^4)mod 11= 3
(7^5)mod 11= 10
(7^6)mod 11= 4
(7^7)mod 11= 6
(7^8)mod 11= 9
(7^9)mod 11= 8
(7^10)mod 11= 1
(7^11)mod 11= 7
```

Alice

Alice and Bob share a prime number q and an integer α, such that $\alpha < q$ and α is a primitive root of q

① $q = 11 \quad \alpha = 7$

Alice generates a private key X_A such that $X_A < q$

② $X_A \Rightarrow 5$

Alice calculates a public key $Y_A = \alpha^{X_A} \bmod q$

③ $Y_A = \alpha^{X_A} \bmod q$
$= 7^5 \bmod 11 = 10$

Alice receives Bob's public key Y_B in plaintext

Alice calculates shared secret key $K = (Y_B)^{X_A} \bmod q$

⑤ $K = (Y_B)^{X_A} \bmod q$,
$= 9^5 \bmod 11 = 1$

Bob

Alice and Bob share a prime number q and an integer α, such that $\alpha < q$ and α is a primitive root of q

Bob generates a private key X_B such that $X_B < q$

② $X_B \Rightarrow 8$

Bob calculates a public key $Y_B = \alpha^{X_B} \bmod q$

③ $Y_B = \alpha^{X_B} \bmod q$
$= 7^8 \bmod 11 = 9$

Bob receives Alice's public key Y_A in plaintext

Bob calculates shared secret key $K = (Y_A)^{X_B} \bmod q$

⑤ $K = (Y_A)^{X_B} \bmod q$,
$= 10^8 \bmod 11$
$= 1$ //

Same

Example 2

Here is an example. Key exchange is based on the use of the prime number $q = 353$ and a primitive root of 353, in this case $\alpha = 3$. A and B select private keys $X_A = 97$ and $X_B = 233$, respectively. Each computes its public key:

A computes $Y_A = 3^{97} \bmod 353 = 40$.

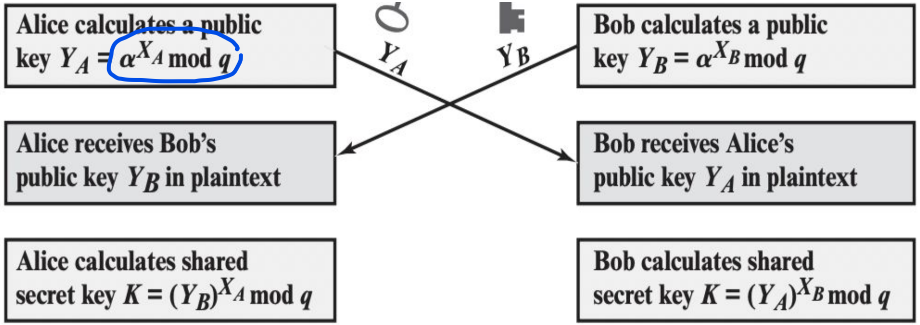
B computes $Y_B = 3^{233} \bmod 353 = 248$.

After they exchange public keys, each can compute the common secret key:

A computes $K = (Y_B)^{X_A} \bmod 353 = 248^{97} \bmod 353 = 160$.

B computes $K = (Y_A)^{X_B} \bmod 353 = 40^{233} \bmod 353 = 160$.

Why both keys are same?



$$
\begin{aligned}
K &= (y_B)^{X_A} \bmod q \quad \checkmark \\
&= (\alpha^{X_B} \bmod q)^{X_A} \bmod q \\
&= (\alpha^{X_B})^{X_A} \bmod q \\
&= (\alpha^{X_A})^{X_B} \bmod q \\
&= (\alpha^{X_A} \bmod q)^{X_B} \bmod q \\
&= (y_A)^{X_B} \bmod q
\end{aligned}
$$

10.1 Alice and Bob use the Diffie–Hellman key exchange technique with a common prime $q = 157$ and a primitive root $\alpha = 5$.

a. If Alice has a private key $X_A = 15$, find her public key Y_A.

b. If Bob has a private key $X_B = 27$, find his public key Y_B.

c. What is the shared secret key between Alice and Bob?

Ans
79
65
78

10.2 Alice and Bob use the Diffie-Hellman key exchange technique with a common prime $q = 23$ and a primitive root $\alpha = 5$.

a. If Bob has a public key $Y_B = 10$, what is Bob's private key Y_B?

b. If Alice has a public key $Y_A = 8$, what is the shared key K with Bob?

c. Show that 5 is a primitive root of 23.


thank you


LIKE
COMMENT
SHARE
SUBSCRIBE

Key points

User A selects a random integer $X_A < q$ and computes $Y_A = \alpha^{X_A} \bmod q$. Similarly, user B independently selects a random integer $X_B < q$ and computes $Y_B = \alpha^{X_B} \bmod q$. Each side keeps the X value private and makes the Y value available publicly to the other side. Thus, X_A is A's private key and Y_A is A's corresponding public key, and similarly for B. User A computes the key as $K = (Y_B)^{X_A} \bmod q$ and user B computes the key as $K = (Y_A)^{X_B} \bmod q$. These two calculations produce identical results:

proof

$$
\begin{aligned}
K &= (Y_B)^{X_A} \bmod q \\
&= (\alpha^{X_B} \bmod q)^{X_A} \bmod q \\
&= (\alpha^{X_B})^{X_A} \bmod q && \text{by the rules of modular arithmetic} \\
&= \alpha^{X_B X_A} \bmod q \\
&= (\alpha^{X_A})^{X_B} \bmod q \\
&= (\alpha^{X_A} \bmod q)^{X_B} \bmod q \\
&= (Y_A)^{X_B} \bmod q
\end{aligned}
$$

Why this is secure?

- Consider an adversary who can observe the key exchange and wishes to determine the secret key K. Because X_A and X_B are private, an adversary only has the following ingredients to work with: q, a, Y_A, and Y_B.
- Thus, the adversary is forced to take a discrete logarithm to determine the key. For example, to determine the private key of user B, an adversary must compute

$$X_B = \mathrm{dlog}_{\alpha,q}(Y_B)$$

The adversary can then calculate the key K in the same manner as user B calculates it. That is, the adversary can calculate K as

$$K = (Y_A)^{X_B} \bmod q$$

The security of the Diffie–Hellman key exchange lies in the fact that, while it is relatively easy to calculate exponentials modulo a prime, it is very difficult to calculate discrete logarithms. For large primes, the latter task is considered infeasible.

i) man-in-the middle

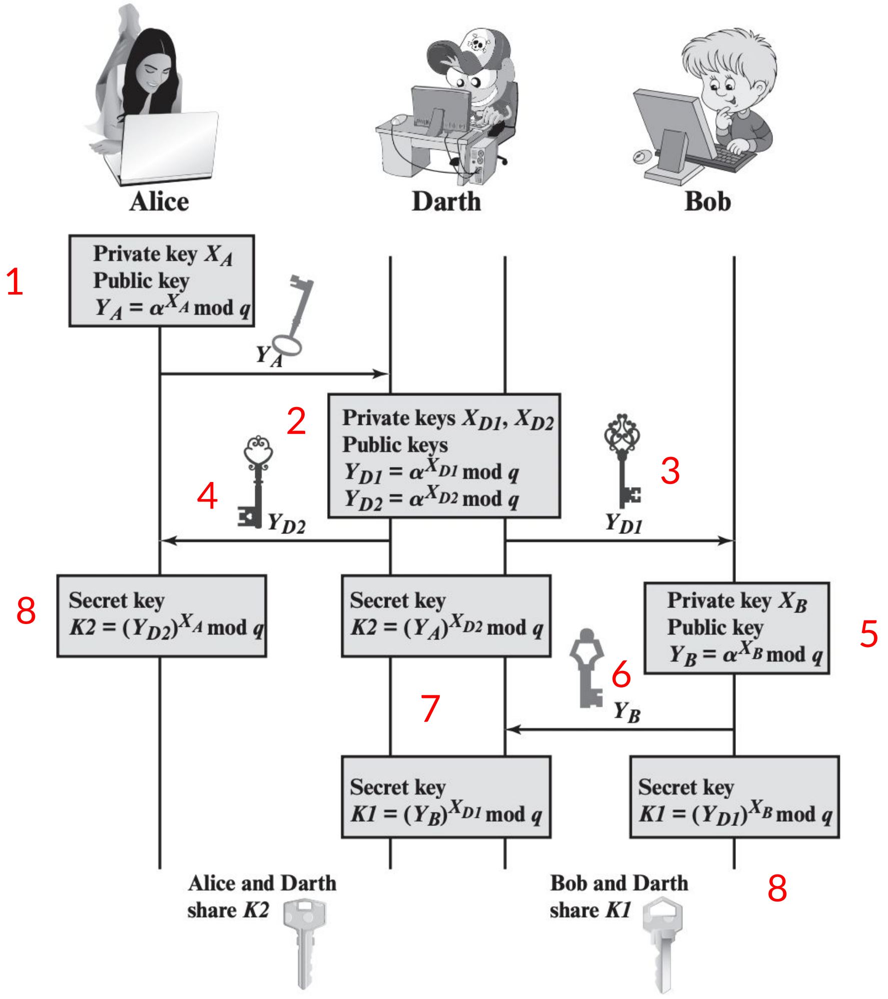


Figure 10.2 Man-in-the-Middle Attack

The protocol depicted in Figure 10.1 is insecure against a man-in-the-middle attack. Suppose Alice and Bob wish to exchange keys, and Darth is the adversary. The attack proceeds as follows (Figure 10.2).

1. Darth prepares for the attack by generating two random private keys X_{D1} and X_{D2} and then computing the corresponding public keys Y_{D1} and Y_{D2}.
2. Alice transmits Y_A to Bob.
3. Darth intercepts Y_A and transmits Y_{D1} to Bob. Darth also calculates $K2 = (Y_A)^{X_{D2}} \bmod q$.
4. Bob receives Y_{D1} and calculates $K1 = (Y_{D1})^{X_B} \bmod q$.
5. Bob transmits Y_B to Alice.
6. Darth intercepts Y_B and transmits Y_{D2} to Alice. Darth calculates $K1 = (Y_B)^{X_{D1}} \bmod q$.
7. Alice receives Y_{D2} and calculates $K2 = (Y_{D2})^{X_A} \bmod q$.

At this point, Bob and Alice think that they share a secret key, but instead Bob and Darth share secret key $K1$ and Alice and Darth share secret key $K2$. All future communication between Bob and Alice is compromised in the following way.

1. Alice sends an encrypted message M: E($K2$, M).
2. Darth intercepts the encrypted message and decrypts it to recover M.
3. Darth sends Bob $E(K1, M)$ or E($K1$, M'), where M' is any message. In the first case, Darth simply wants to eavesdrop on the communication without altering it. In the second case, Darth wants to modify the message going to Bob.


thank you


LIKE
COMMENT
SHARE
SUBSCRIBE