Name: Prem Vinod Bansod
Roll No.: 41310
Assignment No.: 03 (ICS)

Title: Diffie-Hellman key exchange

Problem Statement: To implement a Diffie-Hellman Key Exchange algorithm.

Objective:

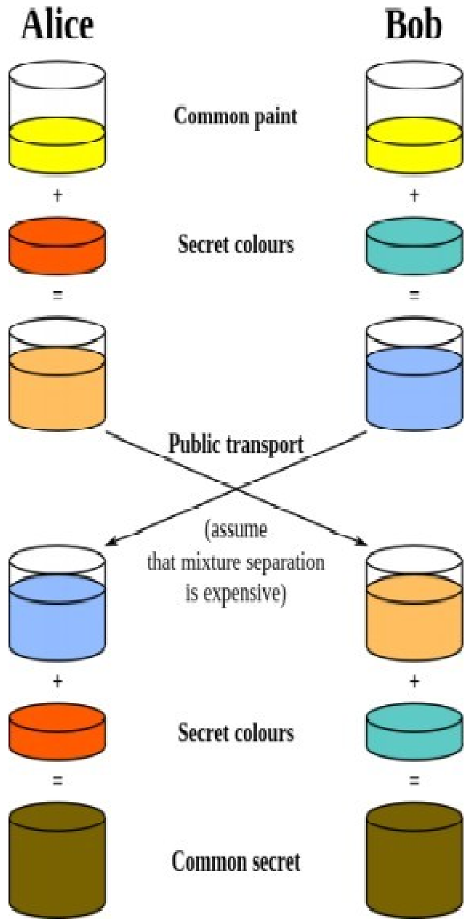
- The Basic Concepts of a Diffie-Hellman key exchange.
- General structure Diffie-Hellman key exchange.
- Logical implementation of Diffie-Hellman key exchange.

Theory:

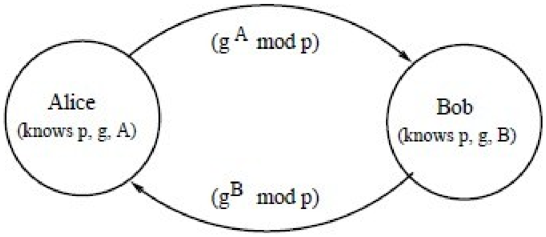
Introduction:

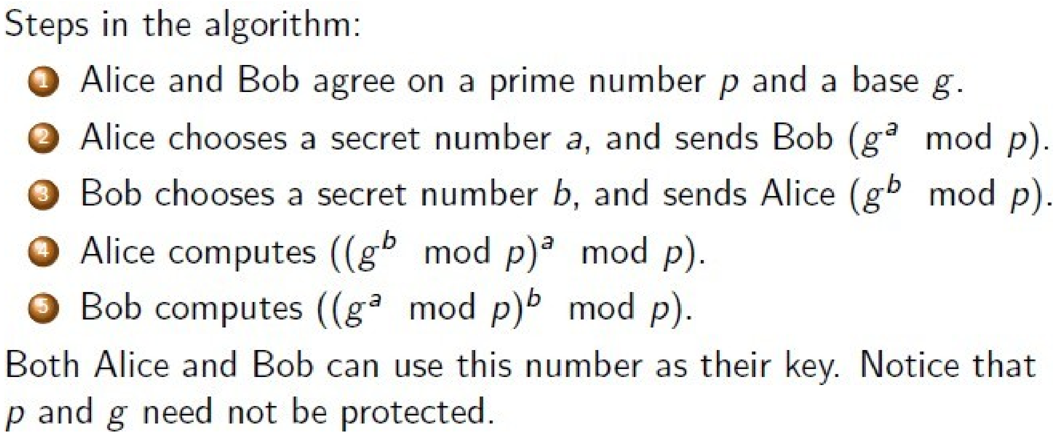
Diffie–Hellman key exchange (DH) is a method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as originally conceptualized by Ralph Merkle and named after Whitfield Diffie and Martin Hellman DH is a mathematical algorithm that permits two PCs to produce an identical shared secret on both systems, despite the fact that those systems might never have communicated with one another. That shared secret can then be utilized to safely exchange a cryptographic encryption key. That key then encrypts traffic between the two systems. Diffie-Hellman is not an encryption mechanism that is we don’t commonly utilize DH to encrypt data. Rather, it is a strategy for secure exchange of the keys that encrypt data.

The following diagram shows the general thought of the key exchange by utilizing colours rather than a large number. The procedure starts by having the two gatherings, Alice and Bob, agree on an arbitrary starting colour that does not should be kept secret; in this example the colour is yellow. Each of them chooses a secret colour - red and aqua respectively - that they keep to themselves. The vital piece of the procedure is that Alice and Bob now combine their secret colour with their commonly shared colour, bringing about orange and blue mixtures respectively, and then freely exchange the two mixed colours. At last, each of the two combine the colour they got from the partner with their own particular private colour. The outcome is a last colour mixture (brown) that is identical with the partner‘s colour mixture.



2. STEPS OF DEFFIE HELLMAN KEY EXCHANGE





Steps in the algorithm:

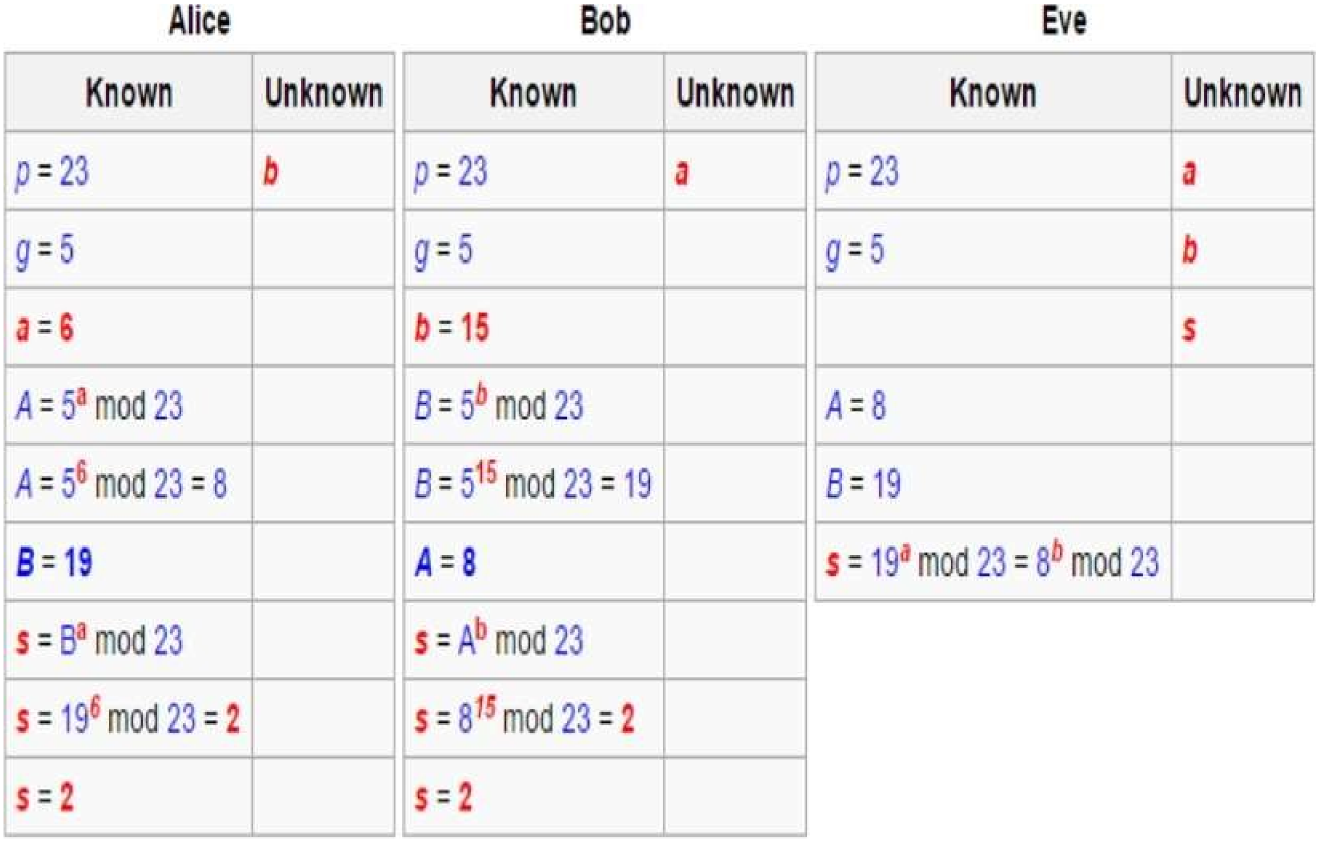
1. Alice and Bob agree on a prime number p and a base g.
2. Alice chooses a secret number a, and sends Bob $(g^a \mod p)$.
3. Bob chooses a secret number b, and sends Alice $(g^b \mod p)$.
4. Alice computes $((g^b \mod p)^a \mod p)$.
5. Bob computes $((g^a \mod p)^b \mod p)$.

Both Alice and Bob can use this number as their key. Notice that p and g need not be protected.

3. EXAMPLE OF DEFFIE HELLMAN KEY EXCHANGE

1. g = public (prime) base, known to Alice, Bob, and Eve.
   g = 5
2. p = public (prime) modulus, known to Alice, Bob, and Eve.
   p = 23
3. a = Alice‘s private key, known only to Alice.
   a = 6
4. b = Bob‘s private key known only to Bob.
   b = 15
5. A = Alice‘s public key, known to Alice, Bob, and Eve.
   A = mod p = 8
6. B = Bob‘s public key, known to Alice, Bob, and Eve.
   B = mod p = 19
7. Alice computes 19 6 mod 23 = 2
8. Bob computes 8 15 mod 23 = 2
9. Then 2 is the shared secret.

Above example is pictorially represented as follows :



Alice

Known	Unknown
$p = 23$	b
$g = 5$	
$a = 6$	
$A = 5^a \bmod 23$	
$A = 5^6 \bmod 23 = 8$	
$B = 19$	
$s = B^a \bmod 23$	
$s = 19^6 \bmod 23 = 2$	
$s = 2$	

Bob

Known	Unknown
$p = 23$	a
$g = 5$	
$b = 15$	
$B = 5^b \bmod 23$	
$B = 5^{15} \bmod 23 = 19$	
$A = 8$	
$s = A^b \bmod 23$	
$s = 8^{15} \bmod 23 = 2$	
$s = 2$	

Eve

Known	Unknown
$p = 23$	a
$g = 5$	b
	s
$A = 8$	
$B = 19$	
$s = 19^a \bmod 23 = 8^b \bmod 23$	

4. SECURITY ISSUE

Man-In-The-Middle Attack:

This algorithm has a noteworthy weakness as man - in - the - middle vulnerability. In this attack, a malicious third party, usually referred to as ―Eve‖ (for ―eavesdropper‖) recovers Alice‘s public key and sends her own public key to Bob. At the point when Bob transmits his public key, Eve interrupts on and substitutes the value with her own public key and after that sends it to Alice. At this point, Alice would have gone to an agreement on a common secret key with Eve rather than Bob and it is feasible for Eve to decrypt any messages conveyed by Alice or Bob, and after that read and perhaps alter them before the re- encryption with the suitable key and transmitting them to alternate party.

This weakness is available on the grounds that Diffie Hellman key exchange does not authenticate the members. Possible solutions include the use of digital signatures and other protocol variants.

5. ADVANTAGES

1. The security factors with respect to the fact that solving the discrete logarithm is very challenging.
2. That the shared key (i.e. the secret) is never itself transmitted over the channel.

6. DISADVANTAGES

1. The fact that there are expensive exponential operations involved, and the algorithm cannot be used to encrypt messages - it can be used for establishing a secret key only.
2. There is also a lack of authentication.
3. There is no identity of the parties involved in the exchange.
4. It is easily susceptible to man-in-the-middle attacks. A third party C, can exchange keys with both A and B, and can listen to the communication between A and B.
5. The algorithm is computationally intensive. Each multiplication varies as the square of n, which must be very large. The number of multiplications required by the exponentiation increases with increasing values of the exponent, x or y in this case.
6. The computational nature of the algorithm could be used in a denial of-service attack very easily.

CONCLUSION: Hence, Diffie-Hellman key exchange algorithm was successfully Implemented.