18 September, 2024

Diffie-Hellman
Primitive Roots
DH Examples
DH and man in the middle attacks
Digital Signatures and Digital Certificates

Diffie-Hellman

- First public key algorithm invented
- Published in 1976
- Specific method for securely exchanging cryptographic keys over a public channel
- Concept given by Ralph Merkle
- Named after Whitfield Diffie and Martin Hellman (British Intelligence Officers)

Note: DH is a public key exchange algorithm, neither encryption nor signature

Diffie-Hellman: Details

Uses modular arithmetic also called the clock arithmetic: g mod p. where g is the generator and p is the prime modulus

$1 < g < p$

g is a primitive root of p

Consider two numbers g & p shared publicly between A & B

A computes $X = g^x \bmod p$ (x is the secret from Alice)

B computes $Y = g^y \bmod p$ (y is the secret from Bob)

Alice & Bob exchange X & Y

A computes $K_{AB} = Y^x \bmod p$

B computes $K_{BA} = X^y \bmod p$

$K_{AB} = K_{BA} = g^{xy} \bmod p$

Primitive Roots

For g to be the primitive root of p, we have to have the following property:

Values g^1 (mod p), g^2 (mod p), ..., g^{p-1} (mod p) should map to all the values in range 1 to (p-1). Here, order is not important, but what is essential is that if we take g to all the different exponential values from 1 to p-1, and apply the modulo p, we should be able to see all the possible values 1 to p-1.

If we take p=11, we can try to see if g=1 works. In class, we saw that when g=1, for all exponents, our answer is 1, so this does not fulfill our requirements.

On the other hand, we saw that when g=2, the successive values of g^1 (mod p), g^2 (mod p), g^3 (mod p), till g^{10} (mod p) resulted in all the values 1 to 10 . Therefore, 2 is a primitive root of 11.

DH Examples:

EXAMPLE 1:

g = 2, p = 11

Alice → x = 8 (secret key)
Bob → y = 4 (secret key)

Alice computes X (public key of Alice) = 2^8 mod 11 = 3
(x, X) = (8, 3)

Bob computes Y (public key of Bob) = 2^4 mod 11 = 5
(y, Y) = (4, 5)

Alice shares X with Bob, Bob shares Y with Alice

K_{AB} = 5^8 mod 11 = 390625 mod 11 = 4

KBA = 3^4 mod 11 = 81 mod 11 = 4

Since they are the same, both users can now use this new key for secured communication later on.

EXAMPLE 2:

g = 3, p = 353

Alice computes secret => x = 97
g^x mod p = 397 mod 353 = 40

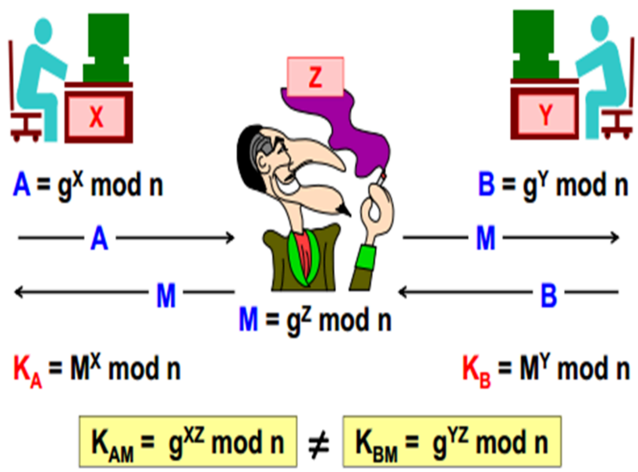
Bob computes secret => y = 233
g^y mod p = 3233 mod 353 = 248

Alice gets 248 from Bob =>
   Alice computes => 24897 mod 353 = 160

Bob gets 40 from Alice =>
   Bob computes => 40233 mod 353 = 160

DH and man in the middle attacks:

If someone can intercept the messages of Alice and Bob and impersonate them, then they may modify the original message by using their own secret key z along with the normal generator g and prime number p. Ultimately, the final keys created at Alice and Bob will not be the same, as seen in this illustration below.



Further Reading on Diffie-Hellman:

[What is the Diffie–Hellman (DH) Algorithm? | Security Encyclopedia (hypr.com)]

Digital Signatures and Digital Certificates (not included in Mid-01 syllabus)

We discussed Digital Signatures.

- Combines a hash with a digital signature algorithm

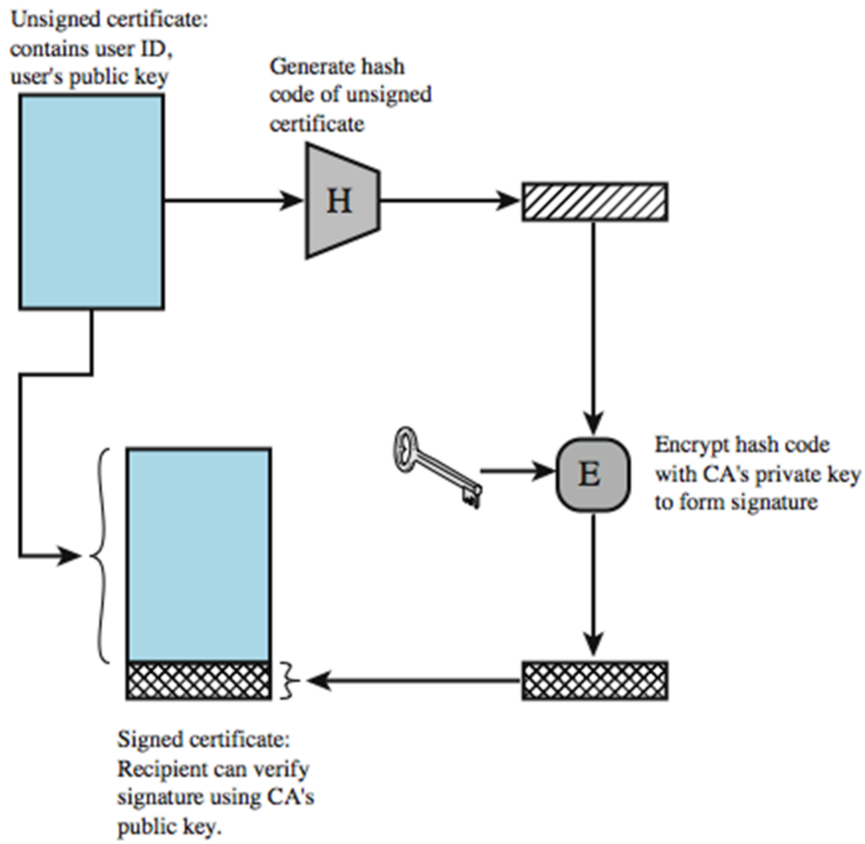
To sign:

- hash the data
- encrypt the hash with the sender's private key
- send data signer's name and signature

To verify:

- hash the data

- find the sender's public key
- decrypt the signature with the sender's public key
- the result of which should match the hash



Certificate Authority (CA):

- A trusted third party - must be a secure server
- Signs and publishes X.509 Identity certificates
- Revokes certificates and publishes a Certification Revocation List (CRL)

Many vendors (CAs) →
- OpenSSL - open source, very simple
- Netscape - free for limited number of certificates
- Entrust - Can be run by enterprise or by Entrust
- Verisign - Run by Verisign under contract to enterprise
- RSA Security - Keon servers