Network Security – Cryptography II

STUDY FOR FE

Public key cryptography

Suppose that two parties have never met each other but they want to communicate securely. They will have to establish a key in order to communicate with each other. Is it possible to establish such a key commonly without ever sharing it over network?

Yes – In 1976, Diffie-Hellman key exchange became the first practical public-key exchange protocols.

Diffie-Hellman Key-Exchange - Basics

The paint analogy

Alice and Bob agree upon a common paint on an insecure network.

Alice and Bob privately select a secret color.

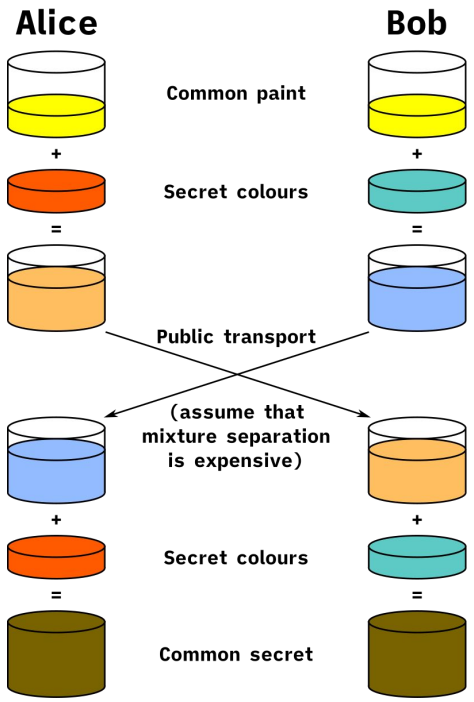
They add their secret colors to the common color in order to create a mixture. It's easy to create a new color by mixing but hard to reverse = 1-way function.

The new mixtures are exchanged publicly over insecure network.

They add their secret colors to these mixtures and create a common secret color.

This common secret color was obtained without any public exchange.

It can serve as an encryption/decryption key!



Diffie-Hellman Key-Exchange - Algorithm

- Publicly pick a prime modulus p and a base generator g (< p) p = 17, g = 6
- g is a primitive root modulo p i.e. g^x mod p will equally likely result in an integer between 0 and p.
- Each party selects a private keys < p -1. Alpha's private key = x = 4, Beta's private key = y = 5
- Each party generates and communicates $g^{private}$ key mod p

Alpha's A = g^x mod p = 6^4 mod 17 = 4

Beta's B = g^y mod p = 6^5 mod 17 = 7

Alpha sends A to Beta and Beta sends B to A.

Alpha's common secret key = B^x mod p = 7^4 mod 17 = 4

Beta's common secret key A^y = 4^5 mod 17 = 4

The trick works because $(g^x \text{ mod } p)^y \text{ mod } p = (g^y \text{ mod } p)^x \text{ mod } p$

Remember, this is simply key exchange. It's not authentication. Neither party knows who they have exchanged keys with! Authentication is required for secure encryption.

Discovering the common secret key even with publicly known details g, p, gx mod p and gy mod p would take longer than the lifetime of universe!

Discrete Logarithm Problem.