Public Key Cryptography

COMP 435
Fall 2017
Prof. Cynthia Sturton

Administrative

- Mandatory office hour visit by 9/27/17
- Assignment 1 due 9/10/17 @ 11:59 PM
- Sign up for Piazza

Public Key vs. Symmetric

Public Key

- public, private keys
- used for authentication, integrity, key distribution
- uses one-way functions

Symmetric

- secret key
- used for confidentiality
- uses substitution and transposition

One Way Function

$33^3 = ?$

One Way Function

33^3 = ?

$\sqrt[3]{35937}$ = ?

$\sqrt[3]{103823}$ = ?

Public Key Encryption for Confidentiality


Alice


Bob

$C = \mathrm{Enc}_{\text{pub-B}}(msg)$

C →

$msg = \mathrm{Dec}_{\text{priv-B}}(C)$

Public Key Encryption for Authentication


Alice


Bob

$C = \mathrm{Enc}_{\text{priv-A}}(msg)$

C →

$msg = \mathrm{Dec}_{\text{pub-A}}(C)$

Properties of Public Key Algorithms

- Given k_{pub} and C, difficult to compute M
- Given k_{pub}, C, and M, difficult to compute k_{priv}

Public Key Algorithms

- RSA
- Diffie-Hellman
- Elliptic Curve Cryptography

Key Exchange

Diffie-Hellman Key Exchange

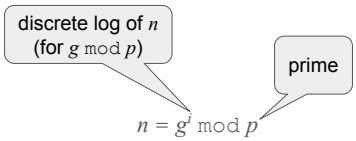
$$n = g^i \bmod p$$

Diffie-Hellman Key Exchange

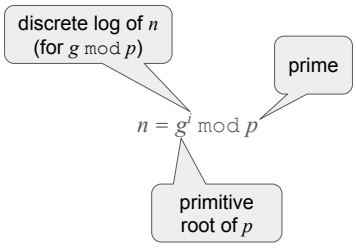
$$n = g^i \bmod p$$

prime

Diffie-Hellman Key Exchange



Diffie-Hellman Key Exchange



$n = g^i \bmod p$

primitive root of p

For all n, $1 \leq n < p$,

there exists exactly one i such that

$$g^i \bmod p = n$$

One-way Function

$$g^i \bmod p = n$$

$$\mathrm{dlog}_{g,p}(n) = i$$

One-way Function

easy to compute

$$\overbrace{g^i \bmod p}^{} = n$$

$$\mathrm{dlog}_{g,p}(n) = i$$

One-way Function

easy to compute

$$\overbrace{g^i \bmod p}^{} = n$$

$$\underbrace{\mathrm{dlog}_{g,p}(n)}_{\text{hard to compute}} = i$$

Diffie-Hellman Key Exchange

Alice

g, p

Bob

$a < p$

$A := g^a \bmod p$

A

B

$b < p$

$B := g^b \bmod p$

$K := B^a \bmod p$

$= (g^b)^a \bmod p$

$= g^{ba} \bmod p$

$K := A^b \bmod p$

$= (g^a)^b \bmod p$

$= g^{ab} \bmod p$

Digital Signatures

Digital Signatures


Alice


Bob

$H := SHA\text{-}256\ (msg)$

$H_k := \mathrm{Enc}_{priv\text{-}A}(H)$

$M := [msg \mid H_k]$

$H := SHA\text{-}256\ (msg)$

$H \stackrel{?}{=} \mathrm{Dec}_{pub\text{-}A}(H_k)$

Certificates