The Diffie-Hellman Algorithm

Overview

- Introduction
- Implementation
- Example
- Applications
- Conclusion

Introduction

- Discovered by Whitfield Diffie and Martin Hellman
  - "New Directions in Cryptography"
- Diffie-Hellman key agreement protocol
  - Exponential key agreement
  - Allows two users to exchange a secret key
  - Requires no prior secrets
  - Real-time over an untrusted network

Introduction

- Security of transmission is critical for many network and Internet applications
- Requires users to share information in a way that others can't decipher the flow of information

"It is insufficient to protect ourselves with laws; we need to protect ourselves with mathematics."

-Bruce Schneier

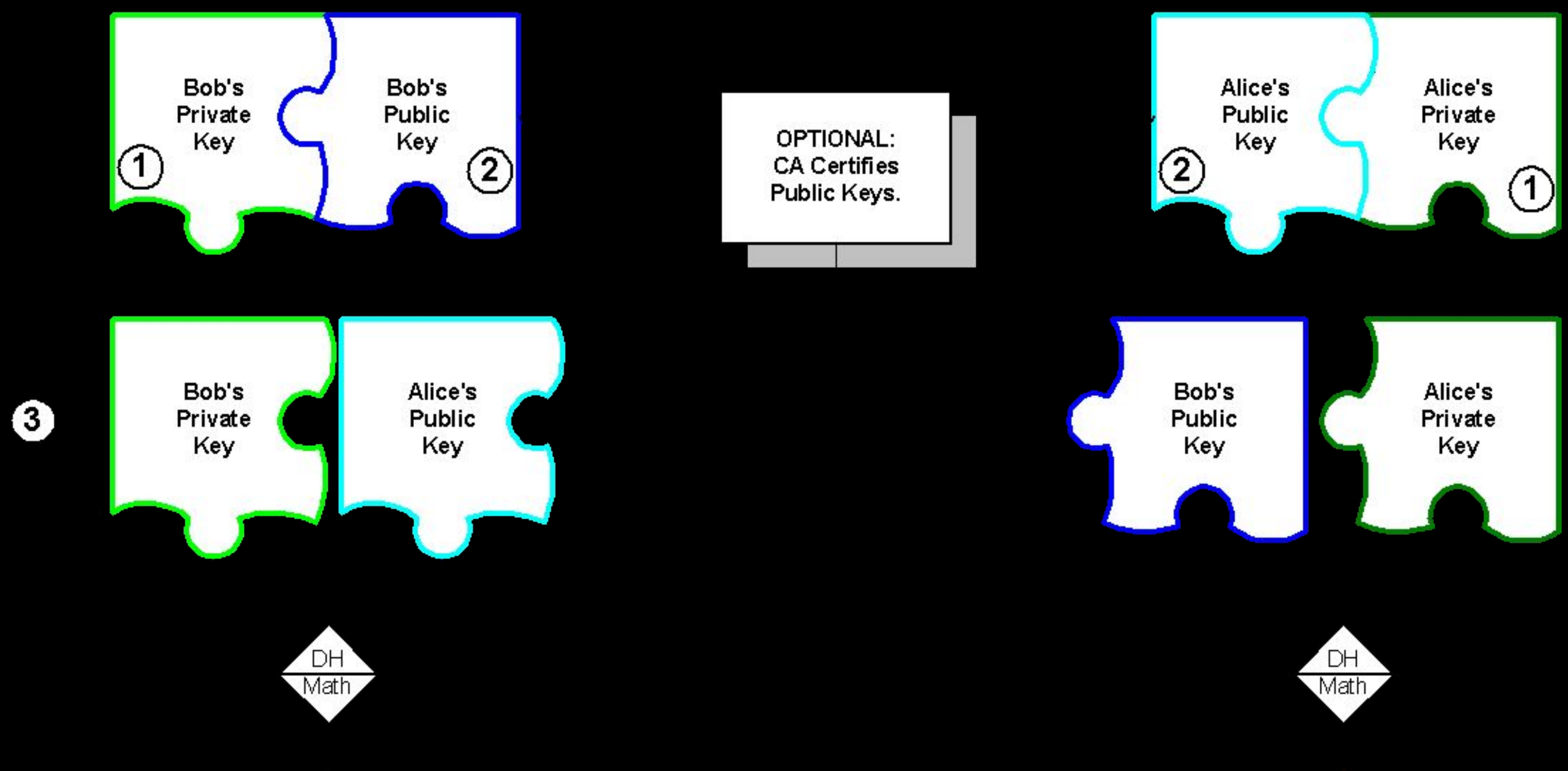
Introduction

- Based on the difficulty of computing discrete logarithms of large numbers.
- No known successful attack strategies*
- Requires two large numbers, one prime (P), and (G), a primitive root of P

Implementation

- P and G are both publicly available numbers
  - P is at least 512 bits
- Users pick private values a and b
- Compute public values
  - $x = g^a \bmod p$
  - $y = g^b \bmod p$
- Public values x and y are exchanged

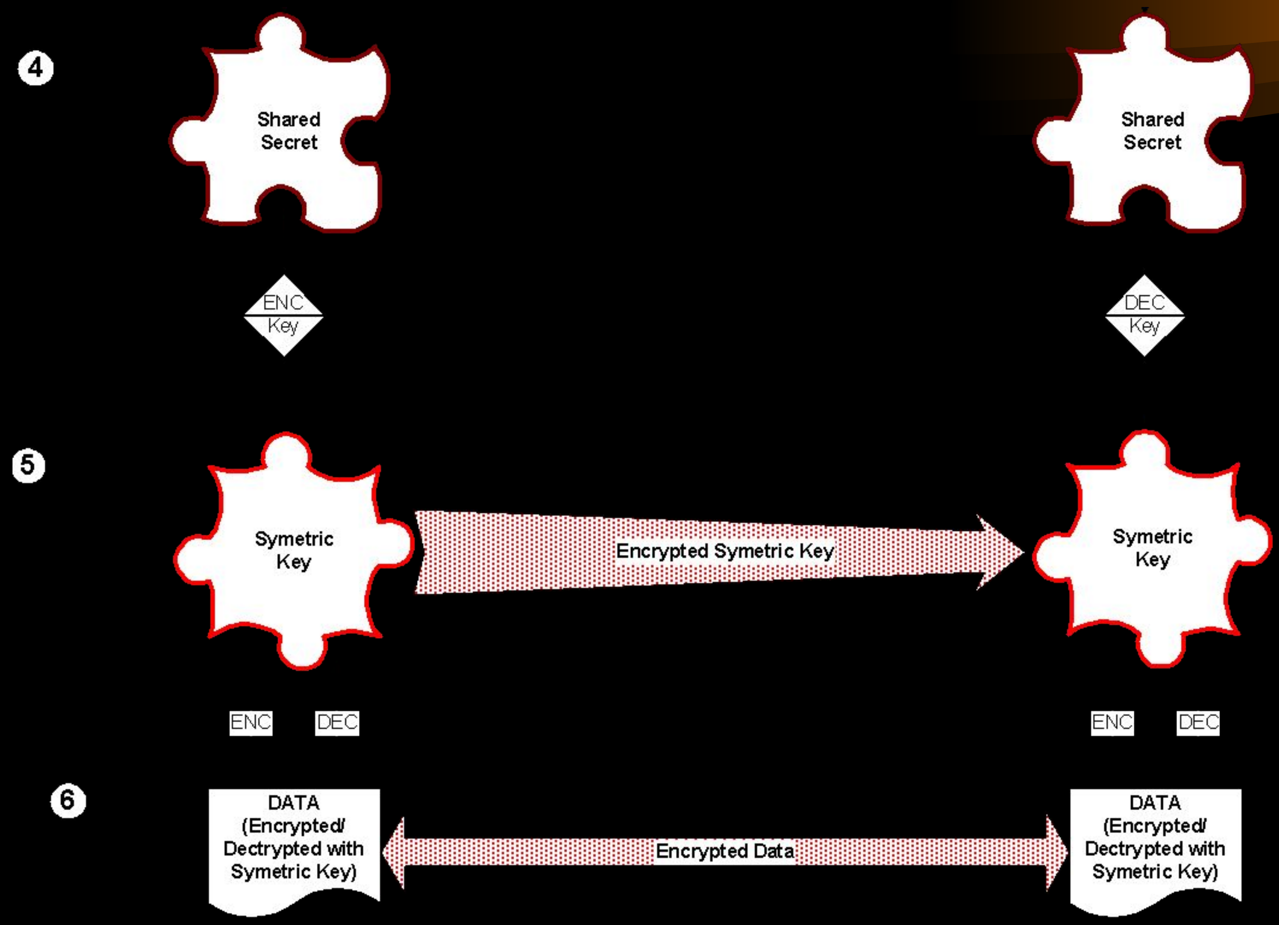
Implementation



Implementation

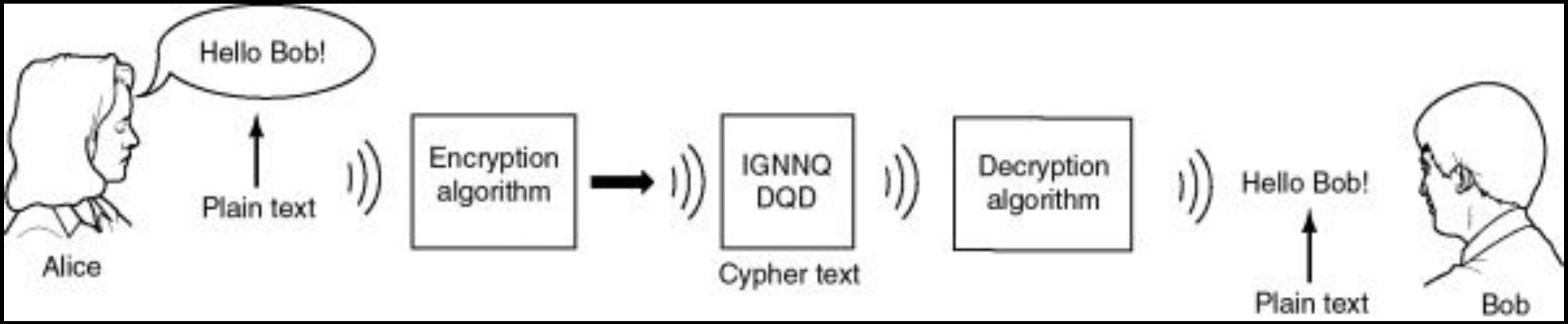
- Compute shared, private key
  - $k_a = y^a \bmod p$
  - $k_b = x^b \bmod p$
- Algebraically it can be shown that $k_a = k_b$
  - Users now have a symmetric secret key to encrypt

Implementation



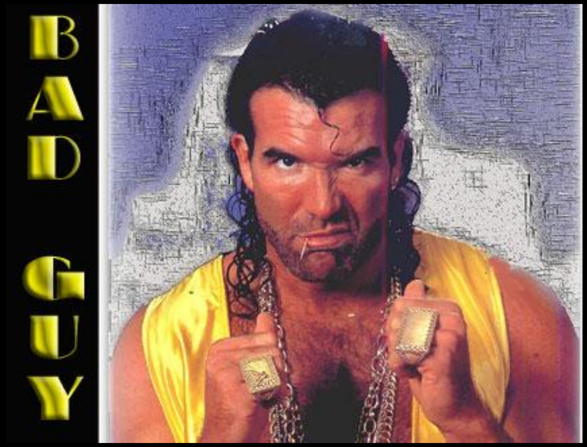
Example

- Two Internet users, Alice and Bob wish to have a secure conversation.
  - They decide to use the Diffie-Hellman protocol



Example

- Bob and Alice are unable to talk on the untrusted network.
  - –Who knows who's listening?

Example

- Alice and Bob get public numbers
  - $P = 23, \; G = 9$
- Alice and Bob compute public values
  - $X = 9^4 \bmod 23 = 6561 \bmod 23 = 6$
  - $Y = 9^3 \bmod 23 = 729 \bmod 23 = 16$
- Alice and Bob exchange public numbers

Example

- Alice and Bob compute symmetric keys
  - $k_a = y^a \bmod p = 16^4 \bmod 23 = 9$
  - $k_b = x^b \bmod p = 6^3 \bmod 23 = 9$
- Alice and Bob now can talk securely!

Example

- If a Diffie-Hellman key exchange is based on prime number 353 and its primitive root is 3. And the two users A &; B using this prime number for key exchange is having secret keys 97 and 233 respectively. A computes Y A as

- P=353, Xa=97, Xb=233,
- Ya=3^97 mod 353
- Yb= 3^233 mod 353
- 3^6 mod 353=729 mod 353=23
- 3^12 mod 353=529 mod 353= 176
- 3^24 mod 353= 30976 mod 353= 265
- 3^48 mod 353= 70225 mod 353=331
- 3^96 mod 353= 109561 mod 353= 131
- 3^97 mod 353= 393 mod 353= 40
- Ya=40

- Yb= 3^233 mod 353
- 3^194 mod 353= 1600 mod 353=188
- 3^218=3^194 * 3^24= 188*265 mod 353
- 49820 mod 353= 47
- 3^230=3^218*3^12 mod 353= 47*176 mod 353= 8272 mod 353 =153
- 3^233 mod 353=153*27 mod 353= 4131 mod 353= 248
- Yb=248
- 3^291 mod 353= (3^194 *3^97) mod 353
- =188*40=7520 mod 353= 107
- 3^291 *3^48= 3^339 mod 353

- Ka=Yb^Xa mod P=248^97 mod 353=160
- Kb=Ya^Xb mod P=40^233 mod 353=
- Ka=248^97 mod 353
- 248^2 %353= 61504%353=82
- 248^4%353= 6724%353=17
- 248^12%353=4913%353=324
- 248^24%353=104976%353=135
- 248^48%353=18225%353=222
- 248^96%353= 49284%353=217
- 248^97%353=53816%353=160

- Kb=Ya^Xb mod P=40^233 mod 353=
- 40^2%353=1600%353=188
- 40^4%353=35344%353=44
- 40^8%353=1936%353=171
- 40^16%353= 29241%353=295
- 40^32%353= 87025%353=187
- 40^64%353=34969%353=22
- 40^128%353=131
- 40^192%353=
- 131*22 %353=2882%353=58
- 40^224%353=187*58%353=256
- 40^232%353=256*171%353=43776%353=4
- 40^233%353=4*40%353=160

Applications

- Diffie-Hellman is currently used in many protocols, namely:
  - Secure Sockets Layer (SSL)/Transport Layer Security (TLS)
  - Secure Shell (SSH)
  - Internet Protocol Security (IPSec)
  - Public Key Infrastructure (PKI)

Conclusion

- Authenticated Diffie-Hellman Key Agreement (1992)
  - Defeats middleperson attack
- Diffie-Hellman POP Algorithm
  - Enhances IPSec layer
- Diffie-Hellman continues to play large role in secure protocol creation

Additional Sources

- http://www.sans.org/rr/encryption/algorithm.php

- http://www.hack.gr/users/dij/crypto/overview/index.html