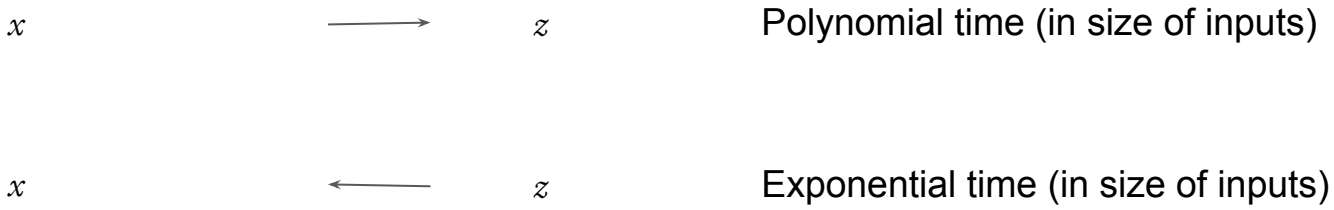
Tutorial 5

Asymmetric Encryption

CS3235 - Spring 2022

One-Way Function



One-Way Function

Polynomial time (in size of inputs)

Exponential time (in size of inputs)

Example: $f(x) = g^x \bmod p$

Group

A group $(G, *)$ is a set G on which a binary operation $*$ is defined that satisfies:

1. **Closure**

   $a * b \in G \qquad \forall \ a, b \in G$

2. **Identity**

   There is an unique identity element e such that

   $e * g = g * e = g \quad \forall \ g \in G$

3. **Inverse**

   $\exists \ g^{-1} \in G$ such that $g * g^{-1} = g^{-1} * g = e \quad \forall \ g \in G$

4. **Associativity**

   for any three $a, b, c \in G$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

Group

Is this a group?

1. The integers Z under addition (+)

2. The integers Z under multiplication (.)

3. The set of complex numbers G = {1, i, −1, −i} under multiplication (.)

Group

Z_N^* Group

- Set of positive integers smaller than and co-prime to integer N
- Group operator is (.) mod N
- $Z_{12}^* = \{1, 5, 7, 11\}$

Z_p^* Group

- Cyclic group if there exists generator g such that $Z_p^* = \{1, g, g^2, \ldots, g^{p-2}\}$

Fermat - Euler

- The inverse of x in Z_N is an element y in Z_N such that $x \cdot y = 1$
- x in Z_N has inverse if and only if $\gcd(x,N) = 1$
- Fermat's theorem:

$$x^{p-1}=1 \ \forall \ x \in Z_p^* \qquad \text{where p is prime}$$

- Euler's generalisation:

$$x^{\Phi(N)}=1 \ \forall \ x \in Z_N^* \qquad \text{where } \Phi(N) = |Z_N^*|$$

Diffie Hellman Key Exchange

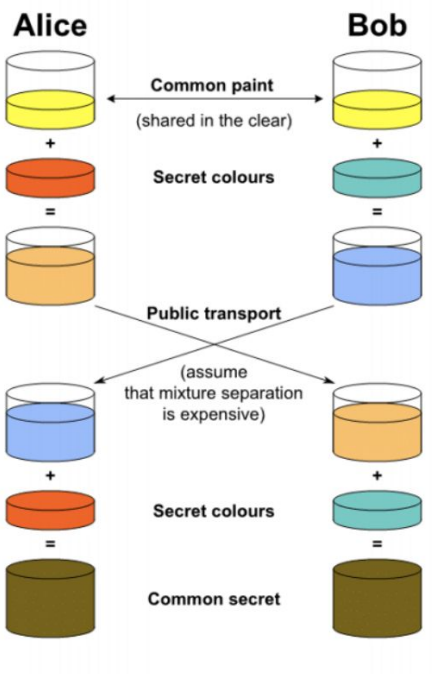


Figure: Diffie Hellman Exchange, Wikipedia

Diffie Hellman Key Exchange

G is a finite cyclic group

$G = \{1, g, g^2, \ldots, g^{n-1}\}$

where g is generator

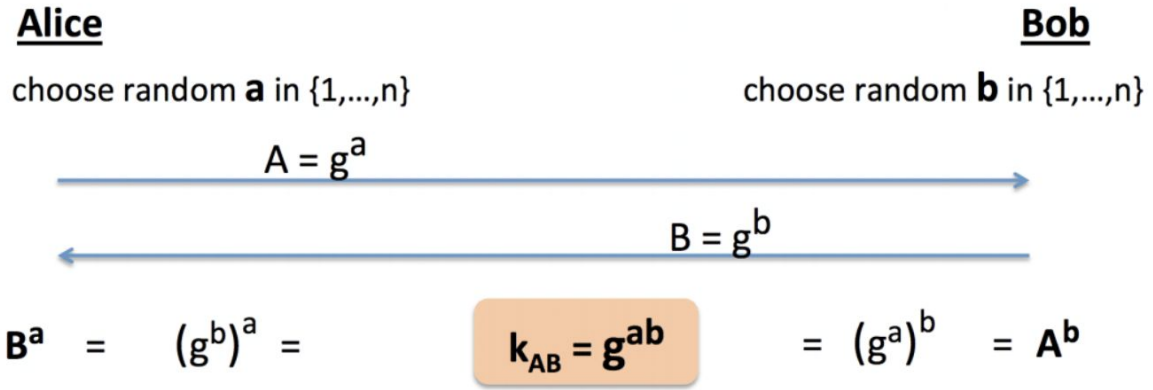


Figure: Diffie Hellman Exchange, Dan Boneh's course

g, g^a, g^b are public

Alice and Bob now have a shared-secret key

Why is Diffie-Hellman Secure?

Given g, g^a, g^b what is g^{ab}?

Define: $DH_g(g^a, g^b) = g^{ab} \ (mod\ p)$

Best algorithm available: General Number Field Sieve (GNFS)

Complexity $\approx O\left(e^{\sqrt[3]{n}}\right)$

What is DH secure against?

Which threat models does DH protect against?

- avesdropper
- ctive Attacker

Public Key Encryption Definitions

Public Key Encryption defined as three algorithms G, E, D:

- G generates key pair (PK, SK)
- E is used to encrypt: $c \leftarrow E(pk,m)$
- D is used to decrypt: $m \leftarrow D(sk,c)$

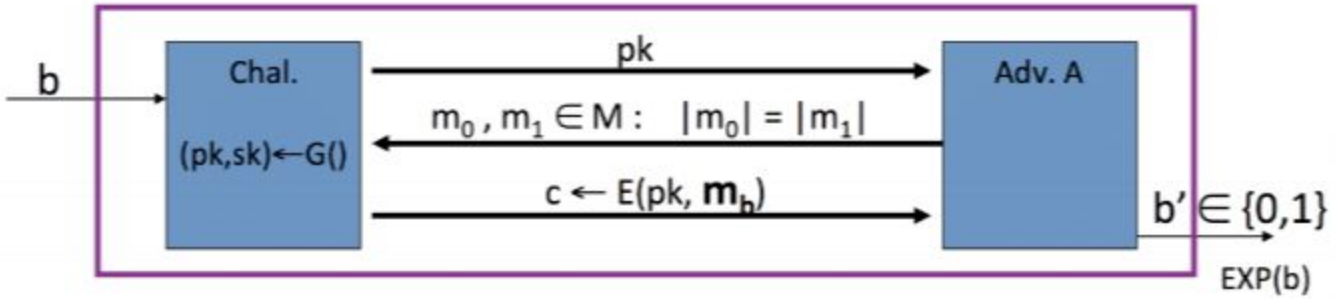
- Relies on the hard problems like factoring and discrete logarithms
- Usually has at least one security parameter

Public Key Use Case

Alice and Bob want to send email in a way that's secure against eavesdropping:

1. Alice generates key pair (pk, sk)
2. Alice sends pk to Bob
3. Bob chooses random x
4. Bob sends y = E(pk, x) to Alice
5. Alice decrypts via D(sk, y) to get x
6. Now both have a shared secret x

Public Key Security: CPA Security



Textbook ElGamal

- **Basis**
  - Large prime p, g is a generator of group Z_p^*
- **Key Generation**
  - Bob selects a private key b in Z_p^*, generates public key $\beta = g^b \bmod p$
  - Publishes (g, p, β) publicly
- **Encryption**
  - Alice chooses a random secret value k and computes $r = g^k \bmod p$
  - Alice computes $t = \beta^k m \bmod p$
  - Ciphertext c = (r,t) sent to Bob
- **Decryption**
  - $D(c, b) = t\, r^{-b} \bmod p = m$

Why is ElGamal Secure?

given B, hard to find secret b

- Same as Diffie-Hellman, called the “Diffie-Hellman Assumption”
- Essentially, given $g^b \bmod p$, very difficult to recover b
- Often called “Discrete Log” problem

Textbook RSA

Key Generation

- Select two large prime numbers p & q, unknown to attacker
- Compute N = pq, $\Phi(N) = (p-1)(q-1)$
- Choose e,d such that $e \cdot d = 1 \bmod \Phi(N)$
- Public key is (e,N) , Private key is (d, N)

Textbook RSA

Encryption

- $E((e, N), m) = m^e \pmod N$

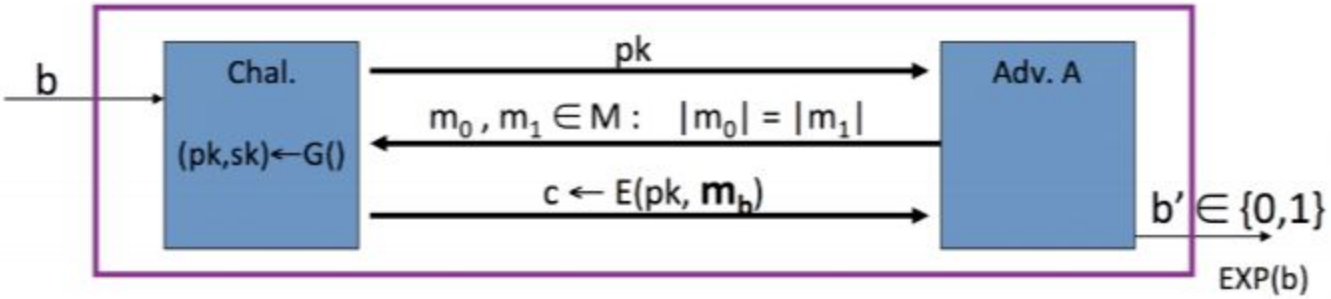
Decryption

- $D((d, N), c) = c^d \pmod N$
- $c^d = (m^e)^d = m^{k\Phi(N) + 1} = m^{k\Phi(N)} \cdot m = m \pmod N$

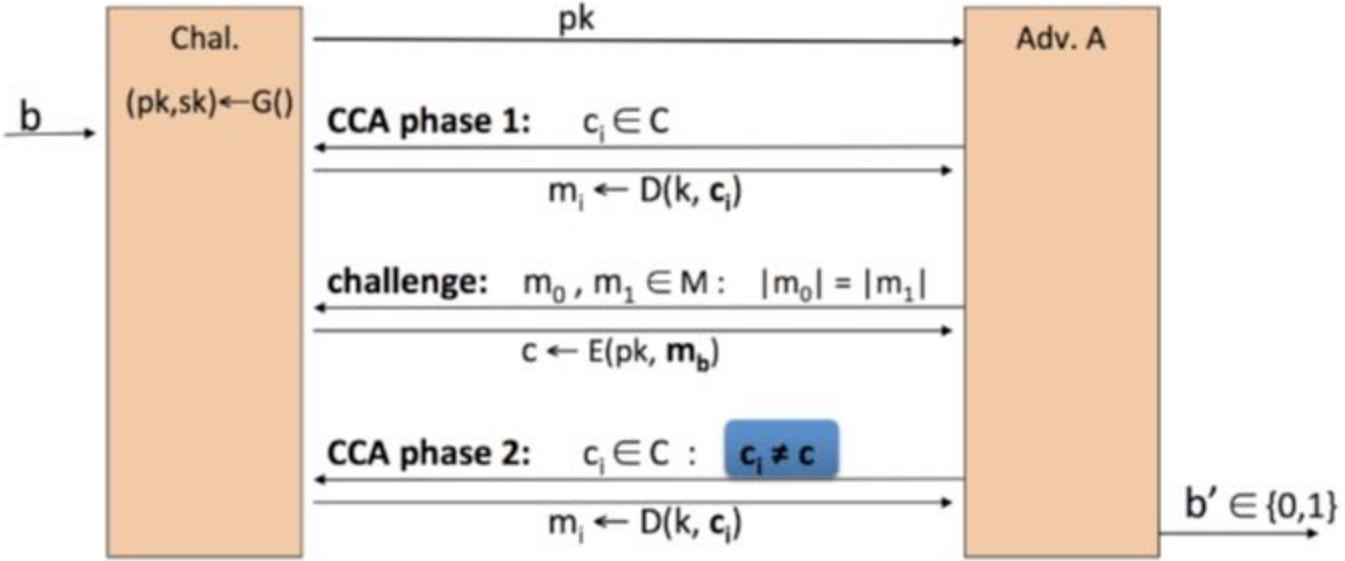
Why is RSA Secure?

- Given (e, N) and c, adversary wants to find *x* such that c = x^e (mod N)
- Basically need to find the “e-th root of c mod N”
- Current state of the art requires factoring N, which is considered hard
  - Again, GNFS, sub-exponential
- Security rests on the idea that time complexity is polynomial for the participants and (sub) exponential for the adversary
- Choose a security parameter big enough that direct attack is not feasible

Is Textbook RSA Semantically Secure?



Is Textbook ElGamal CCA Secure?



Textbook ElGamal Chosen Ciphertext Attack

1. Adversary chooses two distinct values, *m0* and *m1*
2. Sends both in CPA phase, gets back *c* = *(r, t)*
3. Computes *c'* = *(r, 2*t)*, requests that c' be decrypted, gets back *m'*
4. If *m'* = *2 * m0* then b = 0, else b = 1

Adversary wins with advantage 1.0!

Why?

NEVER USE TEXTBOOK ALGORITHMS!

- Use ISO standard implementations when available
- There are *many* variants of all PKE schemes
- Use Public Key Encryption to produce a random shared secret, and then use that to encrypt using strong symmetric ciphers
- Again: never make your own crypto!

Performance Considerations

- PKE is usually orders of magnitude slower than symmetric-key
- PKE usually has limits on size it can encrypt by itself (e.g. 2048 bits)
- Another reason to use PKE to set up SKE only

Kareem’s Homework Tips

- Check your own answers
  - E.g. if asked for a decryption, try to encrypt your answer. Does it match?
- Simplify the question
  - Big numbers are hard to work with. Make a toy version that’s smaller and easier to work with.
- Be careful with answer formats
  - Did the question ask for decimal, hex, or ASCII (text)?

Week 2 Homework Review

1. Each node in the BGP protocol is an ISP or AS. A BGP hijacking attack allows an attacker to (choose the most applicable option):

(1 mark)

- ○ Impersonate a network node
- ○ Perform a “man-in-the-middle” attack by modifying traffic between two nodes
- ○ Route all traffic for a particular network segment through a node they control
- ○ All of the above
- ○ Deny traffic to a network segment
- ○ Eavesdrop on traffic for a network segment

2. IP Spoofing refers to:

(1 mark)

- Modifying IP packet data payload in transit
- Eavesdropping on IP data payload
- None of the above
- Modifying the source address in an IP packet

3. An IP Smurf attack allows an attacker:

(1 mark)

- Eavesdrop on network traffic
- Impersonate another user
- Overload a network node by having other nodes send it large amounts of data
- All of the above
- Modify in-transit network data between a user and a server

4. If an attacker can guess the initial sequence number used by a specific host in TCP, what consequences does this have? Assume the attacker is "off-path", i.e., cannot eavesdrop or intercept packets directly in transit between the host and other nodes. Also the attacker can only guess the sequence number used by a single host, and not other nodes.

(1 mark)

- ○ An attacker can use this to impersonate another node / IP address and receive privileged information sent by the server
- ○ All of the above
- ○ An attacker can use this to force existing (established) TCP sessions to close
- ○ An attacker can use this to intercept an existing (established) TCP session
- ○ An attacker can use this to impersonate another node / IP address and send counterfeit information to the host (server)

5. DNS Cache Poisoning of a specific node allows an off-path network attacker to (choose all that apply):

(1 mark)

- [ ] Impersonate a website
- [ ] Intercept communication between a web server and all users
- [ ] Impersonate a user to a website
- [ ] Intercept communication between a web server and a given client

6. Fill in the blanks

(1 mark)

Consider a stateless network firewall that has an accuracy of 99%. 99% of the legitimate packets are allowed and 99% of malicious packets are dropped. 1,000,000 packets are passed through the firewall of which 100 of the packets are malicious and the rest are not. Answer the following questions:

1. How many malicious packets are dropped by the firewall? 1

2. How many legitimate packets are dropped by the firewall? 2

3. A packet is dropped by the firewall. What is the chance that the packet is actually legitimate (false positive)? 3 %

(Hint: Use the Bayes Rule to calculate 3)

Enter the correct answer below.

1 Please enter a number for this text box.

2 Please enter a number for this text box.

3 Please enter a number for this text box.

7. You have a database of known malware payloads and want to design a firewall that can filter out any packets detected to contain malware. Is it possible to use a stateless firewall to protect against all malware in the database? Briefly explain why or why not.

Does a *stateless* network firewall protect against spoofing internal IP addresses from outside (untrusted) addresses?

Does a *stateless* network firewall protect against an IP smurf attack from outside (untrusted) addresses?

Does a *stateless* network firewall protect against a TCP sequence number prediction attack from outside (untrusted) addresses? Assume that the trusted host impersonated by the attacker is inside the firewall.

Does a *stateless* network firewall protect against a DNS Cache Poisoning attack from outside (untrusted) addresses?

Does a *stateless* network firewall protect against a DNS Cache Poisoning attack from outside (untrusted) addresses?

Does a *stateless* network firewall protect against a BGP route hijacking attack from outside (untrusted) addresses?

Does a *stateless* network firewall protect against application level vulnerabilities?

You’re in charge of protecting your company’s network from outside attackers. Based on the vulnerabilities discussed in class, how do you determine what protections are necessary? What assumption do you make about the attacker?