

D12: Cryptography



Sec 101: MW 3:00-4:00pm DOW 1018

IA: Eric Khiu

Announcement

- ▶ Final Exam Review with Junghwan 4-5pm today DOW1010
- ▶ Extra OH tomorrow June 27 1-3pm DOW1018
- ▶ Final exam Wednesday June 26 8-10am (see Piazza for exam logistics)

Agenda

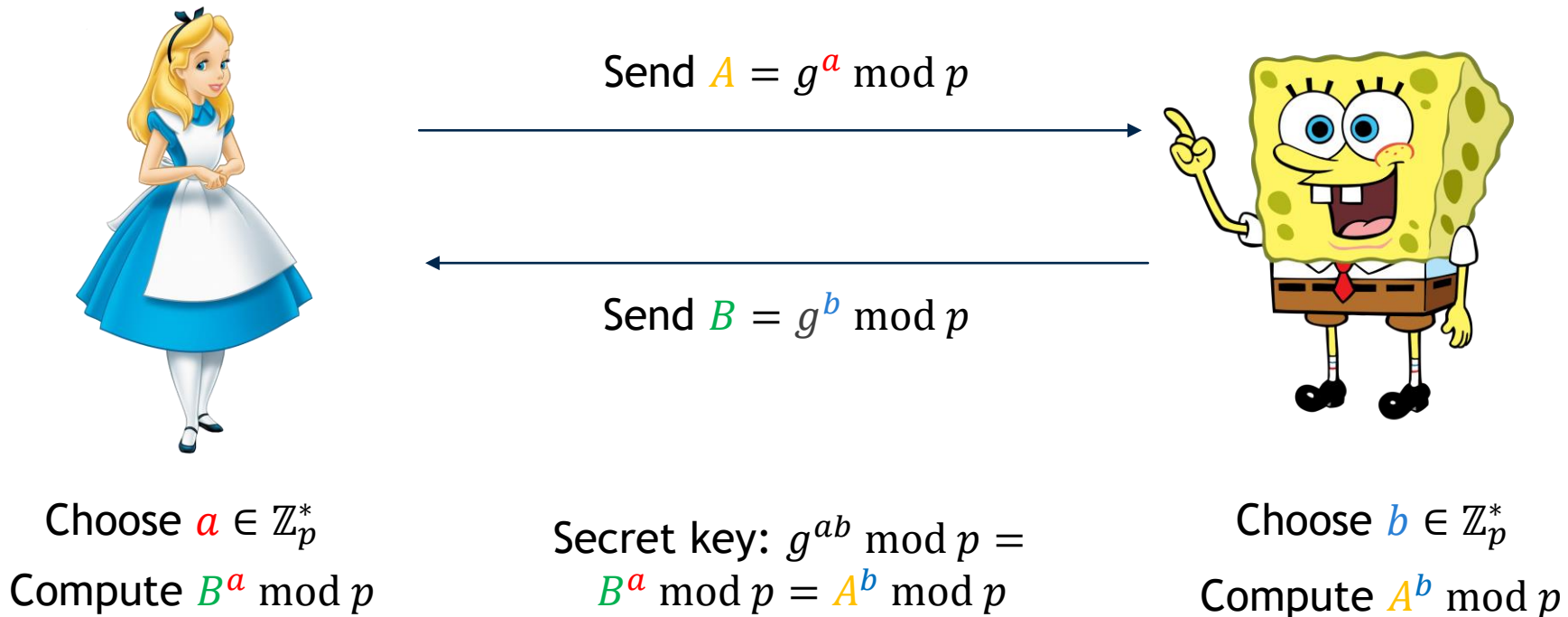
- ▶ Diffie-Hellman Protocol
- ▶ Fermat Little Theorem and Euler's Theorem
- ▶ RSA
- ▶ Cryptography and Complexity

Diffie-Hellman Protocol



Diffie-Hellman Protocol

- ▶ Alice and Bob need a shared secret key in order to encrypt and send messages, but there's an eavesdropper Eve on their communication channel
- ▶ Public information: a prime number p and a generator g



Diffie-Hellman Protocol Example

- ▶ Suppose the prime is $p = 7$ and the generator is $g = 3$
- ▶ Suppose you were Alice and you pick $a = 3$, what do you send to Bob?
 - ▶ $A = 3^3 \bmod 7 = 27 \bmod 7 = 6$
- ▶ After sending A to Bob, suppose you receive $B = 2$, what is the shared key?
 - ▶ $B^a = 2^3 = 8 \equiv 1 \pmod{p}$

Diffie-Hellman Protocol:

- Alice chooses some secret $a \leftarrow \mathbb{Z}_p^*$ at random
- Bob chooses some secret $b \leftarrow \mathbb{Z}_p^*$ at random
- Alice sends $A = g^a \bmod p$ to Bob
- Bob sends $B = g^b \bmod p$ to Alice
- Alice computes $B^a = g^{ab} \bmod p$ as the secret key
- Bob computes $A^b = g^{ab} \bmod p$ as the secret key

FLT and Euler's Theorem



Fermat's Little Theorem

- For a prime number p and any $a, k \in \mathbb{Z}$:

$$a^{1+k(p-1)} \equiv a \pmod{p}$$

- **Example:** Compute $5^{376185} \bmod 376183$ (Hint: 376183 is prime)

$$376185 = 1 + 1(376183 - 1) + 2$$

Here, we have $p = 376183$, $k = 1$, and $a = 5$. Applying Theorem 2.2.2,

$$\begin{aligned} 5^{376185} &\equiv 5^{1+1(376183-1)+2} \pmod{376183} \\ &\equiv 5^{1+1(376183-1)} \cdot 5^2 \pmod{376183} \\ &\equiv 5 \cdot 5^2 \pmod{376183} \\ &\equiv 125 \pmod{376183} \end{aligned}$$

Remark on FLT

- In the current version of course notes (and some books), the FLT is written as

Theorem 236 (Fermat's Little Theorem)

Let p be a prime number. Let a be any element of \mathbb{Z}_p^+ , where

$$\mathbb{Z}_p^+ = \{1, 2, \dots, p-1\}$$

Then $a^{p-1} \equiv 1 \pmod{p}$.

- We can derive our version of FLT easily as follows:

Proof. By FLT, we know $a^{p-1} \equiv 1 \pmod{p}$. Thus, raising 1 to any power k still results in 1:

$$(a^{p-1})^k \equiv 1^k \equiv 1 \pmod{p}$$

Multiply both sides by a ,

$$a \cdot (a^{p-1})^k \equiv a \cdot 1 \pmod{p}$$

$$a^{1+k(p-1)} \equiv a \pmod{p}$$

Euler's Theorem

- For any integers a, k , and $n = pq$, where p and q are **distinct** primes

$$a^{1+k(p-1)(q-1)} \equiv a \pmod{n}$$

- **Example:** Compute $5^{376376} \pmod{35}$

$$(p-1)(q-1) = 6 \cdot 4 = 24$$

From here, we apply repeated squaring:

$$\begin{aligned} 5^{376376} &\equiv 5^{15682 \cdot 24 + 1 + 7} \pmod{35} \\ &\equiv 5^{15682 \cdot 24 + 1} \cdot 5^7 \pmod{35} \\ &\equiv 5 \cdot 5^7 \pmod{35} \\ &\equiv 5^8 \pmod{35} \end{aligned}$$

$$\begin{aligned} 5^1 &\equiv 5 \pmod{35} \\ 5^2 &\equiv 5^2 \equiv 25 \pmod{35} \\ 5^4 &\equiv 25^2 \equiv 625 \equiv 30 \pmod{35} \\ 5^8 &\equiv 30^2 \equiv 900 \equiv 25 \pmod{35} \end{aligned}$$

RSA



Recap: Modular Inverse

- ▶ We say a^{-1} is the **modular (multiplicative) inverse** of a in mod n if

$$a^{-1} \cdot a \equiv 1 \pmod{n}$$

- ▶ Or equivalently, there exists some integer k such that

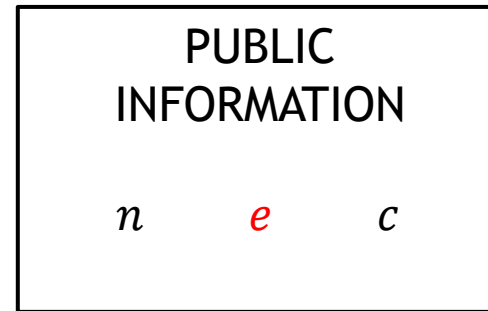
$$a^{-1} \cdot a = 1 + kn$$

- ▶ a has modular inverse in n iff a and n are **coprime**, i.e., $\gcd(a, n) = 1$
- ▶ If p is **prime**, then **all** $x \in \{1, 2, \dots, p - 1\}$ has a modular inverse
- ▶ We can find the modular inverse using **Extended Euclid Algorithm**

Euler's Theorem: For any integers a, k , and $n = pq$, where p and q are *distinct* primes

$$a^{1+k(p-1)(q-1)} \equiv a \pmod{n}$$

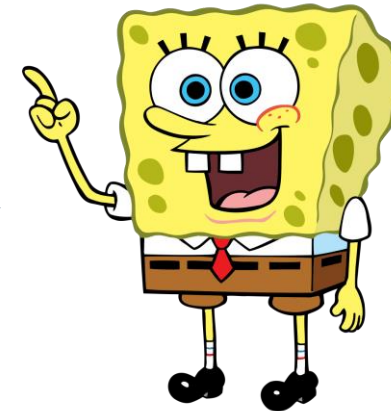
RSA Protocol



Send $c = m^e \pmod{n}$

Compute $m' \equiv c^d \pmod{n}$

$$\begin{aligned} &\equiv (m^e)^d \pmod{n} \\ &\equiv m^{1+k(p-1)(q-1)} \pmod{n} \\ &\equiv m \pmod{n} \end{aligned}$$



Want to send m

Compute $c = m^e \pmod{n}$

Choose p, q , compute n

Find (e, d) :

$$e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$$

$$\Rightarrow e \cdot d = 1 + k(p-1)(q-1)$$

RSA Encryption Example

- ▶ Alice performs several computations
 - ▶ Pick $p = 11$ and $q = 13$
 - ▶ Compute $n = 11 \cdot 13 = 143$
 - ▶ Compute $(p - 1)(q - 1) = 10 \cdot 12 = 120$
 - ▶ Pick $e = 17$, run $\text{ExtendEuclid}(17, 120)$ and get $d = 113$
 - ▶ Publicly broadcast n and e
- ▶ Bob wants to send $m = 5$
 - ▶ Compute $m^e \bmod n = 5^{17} \bmod 143 = 135$ and send to Alice
- ▶ Alice computes $m' = c^d = 135^{113} \bmod 143 = 5$

RSA Protocol

A: Choose p, q , compute $n = pq$

A: Find (e, d) : $e \cdot d \equiv 1 \pmod{(p - 1)(q - 1)}$

A: Broadcast n and e

B: Want to send m

B: Send $c = m^e \bmod n$ to A

A: Compute $c^d \equiv m \bmod n$

PUBLIC
INFORMATION

n

e

c

RSA Encryption Security

- Suppose you were Eve and you want to find m

Poll: Which of the following information would allow you to decrypt the message? (select all apply)

- A. The product $(p - 1)(q - 1)$
- B. p and q individually
- C. A k that satisfies $e \cdot d = 1 + k(p - 1)(q - 1)$

- Ans: All of the above! Key: You just need d

- A. If you have $(p - 1)(q - 1)$, you can run Extended Euclid Algorithm to find d
- B. If you have p and q , you can compute $(p - 1)(q - 1) \rightarrow$ Case A
- C. We can express p and q in terms of k and n (see WS problem 5) \rightarrow Case B

RSA Protocol

A: Choose p, q , compute $n = pq$

A: Find (e, d) : $e \cdot d \equiv 1 \pmod{(p - 1)(q - 1)}$

A: Broadcast n and e

B: Want to send m

B: Send $c = m^e \pmod n$ to A

A: Compute $c^d \equiv m \pmod n$

PUBLIC
INFORMATION

n

e

c

Euler's Theorem: For any integers a, k , and $n = pq$, where p and q are *distinct* primes

RSA Signature

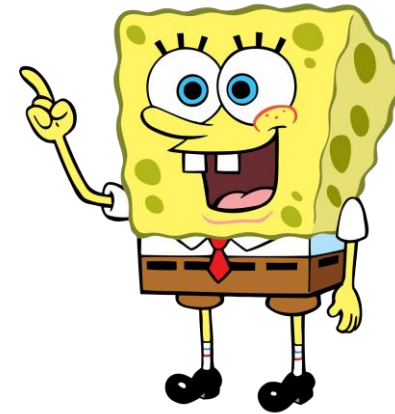
$$a^{1+k(p-1)(q-1)} \equiv a \pmod{n}$$

- Now suppose Alice wants to send a message rather than receiving a message, she wants to have people validate that it came from her



Want to send m
Compute $s = m^d \pmod{n}$

Send (m, s)



Verify: $s^e \equiv (m^d)^e \pmod{n}$
 $\equiv m^{1+k(p-1)(q-1)} \pmod{n}$
 $\equiv m \pmod{n}$

Choose p, q , compute n

Find (e, d) :

$$e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$$

$$\Rightarrow e \cdot d = 1 + k(p-1)(q-1)$$

PUBLIC
INFORMATION

n e

RSA Signature Exercise

Prof. Wein is sending exam questions to the EECS 376 course staff. To ensure that the staff can verify the questions have not been altered, she uses an RSA-based signature scheme with $n = 55$ and public key $e = 27$. What would the signed message (m, s) be, if $m = 52$?

Hint: First find the prime factorization of n

$5 \cdot 11 = 55$ is the only prime factorization!

$$(p - 1)(q - 1) = 4 \cdot 10 = 40$$

RSA Signature

A: Choose p, q , compute $n = pq$

A: Find (e, d) : $e \cdot d \equiv 1 \pmod{(p - 1)(q - 1)}$

A: Broadcast n and e

PUBLIC
INFORMATION

n e

A: Want to send m

A: Compute $s = m^d \pmod n$ and send to B

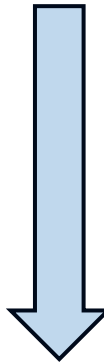
B: Verify if $s^e \equiv m \pmod n$

```
1: function EXTENDED_EUCLID( $x, y$ )
2:   if  $y = 0$  then
3:     return ( $x, 1, 0$ )
4:   else
5:     Write  $x = qy + r$  for an integer  $q$ , where  $0 \leq r < y$ 
6:      $(g, a', b') \leftarrow \text{EXTENDED\_EUCLID}(y, r)$ 
7:      $a \leftarrow b'$ 
8:      $b \leftarrow a' - b'q$ 
9:     return ( $g, a, b$ )
```

Step 1: Find modular inverse

```
1: function EXTENDED_EUCLID( $x, y$ )
2:   if  $y = 0$  then
3:     return ( $x, 1, 0$ )
4:   else
5:     Write  $x = qy + r$  for an integer  $q$ , where  $0 \leq r < y$ 
6:      $(g, a', b') \leftarrow \text{EXTENDED\_EUCLID}(y, r)$ 
7:      $a \leftarrow b'$ 
8:      $b \leftarrow a' - b'q$ 
9:     return ( $g, a, b$ )
```

► We have $(p - 1)(q - 1) = 40$, $e = 27$, we want to find d



x	y	q	r	g	$a \leftarrow b'$	$b \leftarrow a' - b'q$
40	27					

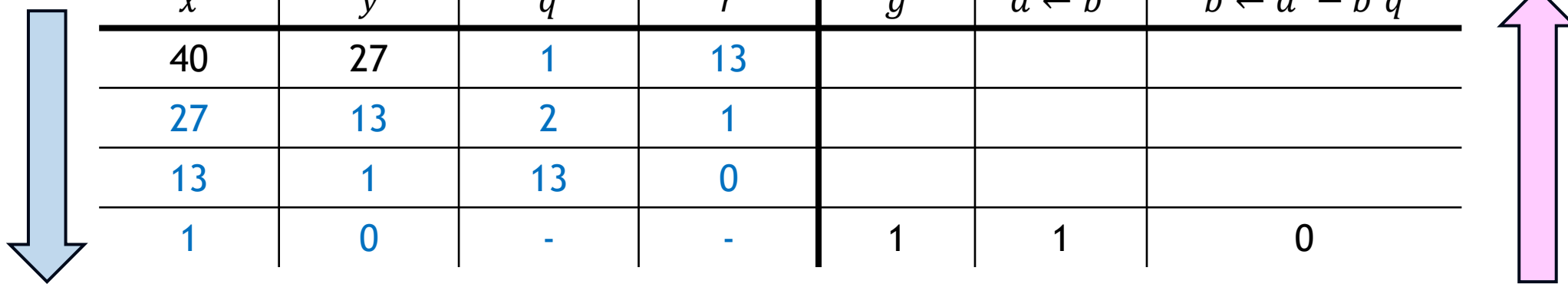
Step 1: Find modular inverse

```

1: function EXTENDED_EUCLID( $x, y$ )
2:   if  $y = 0$  then
3:     return ( $x, 1, 0$ )
4:   else
5:     Write  $x = qy + r$  for an integer  $q$ , where  $0 \leq r < y$ 
6:      $(g, a', b') \leftarrow \text{EXTENDED\_EUCLID}(y, r)$ 
7:      $a \leftarrow b'$ 
8:      $b \leftarrow a' - b'q$ 
9:     return ( $g, a, b$ )

```

► We have $(p - 1)(q - 1) = 40$, $e = 27$, we want to find d



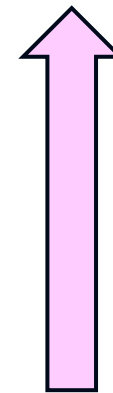
x	y	q	r	g	$a \leftarrow b'$	$b \leftarrow a' - b'q$
40	27	1	13			
27	13	2	1			
13	1	13	0			
1	0	-	-	1	1	0

Step 1: Find modular inverse

```
1: function EXTENDED_EUCLID( $x, y$ )
2:   if  $y = 0$  then
3:     return  $(x, 1, 0)$ 
4:   else
5:     Write  $x = qy + r$  for an integer  $q$ , where  $0 \leq r < y$ 
6:      $(g, a', b') \leftarrow \text{EXTENDED\_EUCLID}(y, r)$ 
7:      $a \leftarrow b'$ 
8:      $b \leftarrow a' - b'q$ 
9:     return  $(g, a, b)$ 
```

► We have $(p - 1)(q - 1) = 40$, $e = 27$, we want to find d

x	y	q	r	g	$a \leftarrow b'$	$b \leftarrow a' - b'q$
40	27	1	13	1	-2	$1 - (-2)(1) = 3$
27	13	2	1	1	1	$0 - (1)(2) = -2$
13	1	13	0	1	0	$1 - (0)(13) = 1$
1	0	-	-	1	1	0



Step 2: Modular Exponentiation

- ▶ Now we have $m = 52$ and $d = 3$. We want to compute $m^d \bmod n = 52^3 \bmod 55$
 - ▶ Hint: $52 \equiv -3 \pmod{55}$
 - ▶ $52^3 \bmod 55 = (-3)^3 \bmod 55 = -27 \bmod 55 = 28$

RSA Signature

A: Choose p, q , compute $n = pq$

A: Find (e, d) : $e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$

A: Broadcast n and e

PUBLIC
INFORMATION

A: Want to send m

A: Compute $s = m^d \bmod n$ and send to B

B: Verify if $s^e \equiv m \pmod{n}$

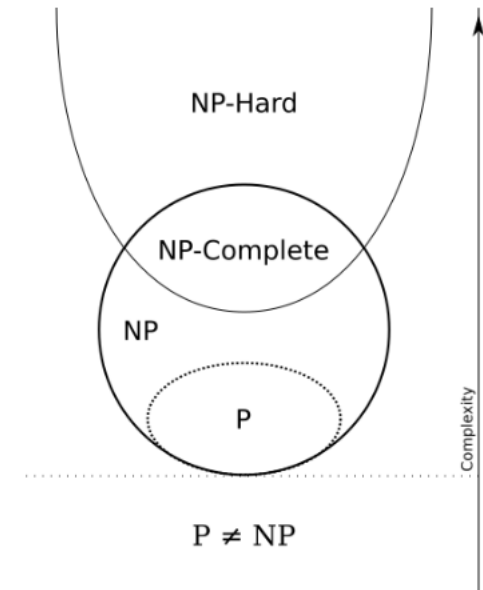
n e

Cryptography and Complexity



Cryptography and NP-Completeness

- ▶ RSA and Diffie-Hellman both rely the problems of integer factorization and discrete log, respectively
- ▶ These problems are thought to be difficult
 - ▶ They're in NP, but are not known to be NP-Hard
 - ▶ If $P \neq NP$, there must be languages between P and NP-Complete
 - ▶ This class is called **NP-Intermediate**
- ▶ DLOG is *expected* to be NP-Intermediate



Thanks for a great semester

- ▶ Consider the following classes to learn more about these topics
 - ▶ Algorithms: EECS 477, CSE 486
 - ▶ Complexity: CSE 574
 - ▶ Randomness: CSE 572
 - ▶ Cryptography: EECS 475, CSE 575
 - ▶ Check the EECS 498/598 list!
- ▶ Good luck on the final!