CSE 484 / CSE M 584
Computer Security: More Cryptography

TA: Jared Moore

jlcmoore@cs

Logistics

- Homework #2 out now (crypto), due on 11/3 8pm.

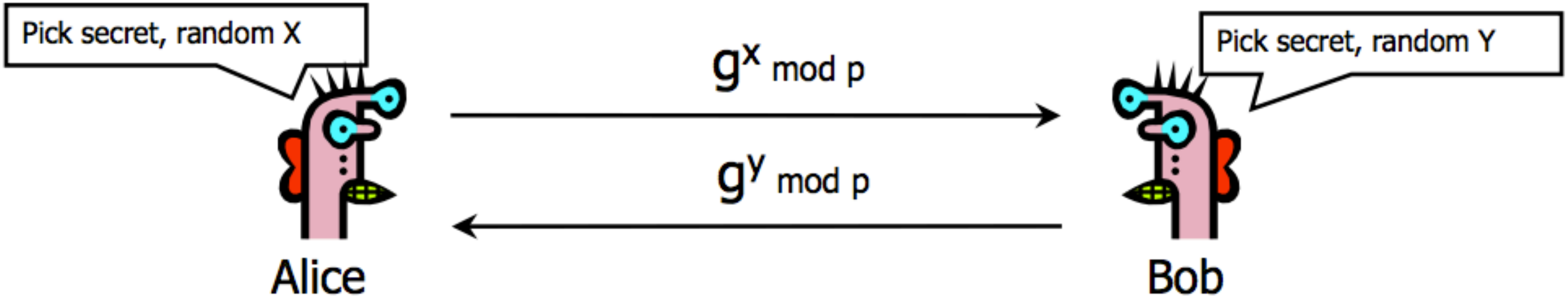
Some Number Theory Facts

- Euler totient function $\varphi(n)$ $(n \geq 1)$ is the number of integers in the $[1,n]$ interval that are relatively prime to n
  - Two numbers are relatively prime if their greatest common divisor (gcd) is 1
  - Easy to compute for primes: $\varphi(p) = p-1$
  - Note that $\varphi(ab) = \varphi(a)\ \varphi(b)$

- Euler's theorem: if $a \in Z_n^*$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$

  Z_n^*: integers relatively prime to n

DH Summary



Pick secret, random X

Pick secret, random Y

g^x mod p

g^y mod p

Alice

Bob

Compute $k=(g^y)^x=g^{xy}$ mod p

Compute $k=(g^x)^y=g^{xy}$ mod p

- Public info: p (large prime) and
  g (generator of Z_p*)

$Z_p^*=\{1, 2 \ldots p-1\}$; $\forall a \in Z_p^*$ $\exists$ i such that $a \equiv g^i$ (mod p)

RSA Cryptosystem [Rivest, Shamir, Adleman 1977]

- Key generation:
  - Generate large primes p, q
    - Say, 1024 bits each (need primality testing, too)
  - Compute **n**=pq and **φ(n)**=(p-1)(q-1)
  - Choose small e, relatively prime to φ(n)
    - Typically, e=3 or $e=2^{16}+1=65537$
  - Compute unique d such that ed ≡ 1 mod φ(n)
    - Modular inverse: $d \equiv e^{-1} \bmod \varphi(n)$

How to compute?

  - Public key = (e,n); private key = (d,n)
- Encryption of m: $c = m^e \bmod n$
- Decryption of c: $c^d \bmod n = (m^e)^d \bmod n = m$

Why RSA Decryption Works

$e \cdot d \equiv 1 \pmod{\varphi(n)}$, thus $e \cdot d = 1 + k \cdot \varphi(n)$ for some k

Let m be any integer in Z_n* (not all of Z_n)

$c^d \bmod n = \mathbf{(m^e)^d} \bmod n \ \mathbf{= m^{1+k \cdot \varphi(n)}} \bmod n$

$= (\mathbf{m} \bmod n) * (\mathbf{m^{k \cdot \varphi(n)}} \bmod n)$

Recall: Euler's theorem: if $a \in Z_n^*$, then $a^{\varphi(n)} = 1 \bmod n$

$c^d \bmod n = (\mathbf{m} \bmod n) * (\mathbf{1} \bmod n)$

$= \mathbf{m} \bmod n$

Proof omitted: True for all m in Z_n, not just m in Z_n*

RSA Encryption Caveats

- Encrypted message needs to be interpreted as an integer less than n
- Don't use RSA **directly** for privacy – output is deterministic! Need to pre-process input somehow
- Plain RSA also does not provide integrity
  - Can tamper with encrypted messages

In practice, OAEP is used: instead of encrypting M, encrypt $M \oplus G(r) ; r \oplus H(M \oplus G(r))$

- r is random and fresh, G and H are hash functions

Read the paper!

- https://people.csail.mit.edu/rivest/Rsapaper.pdf

Sample RSA Decryption

- 26 2 15 13   7 14 13 13 1 28 14   15 13 14 20 9 6 31 25 26 14 16   23 15 26 2   6 13 1
- p=3, q=11, n=33, e=7, d=3

- A-1 B-2 C-3 D-4 E-5 F-6 G-7 H-8 I-9 J-10 K-11 L-12 M-13 N-14 O-15 P-16 Q-17 R-18 S-19 T-20 U-21 V-22 W-23 X-24 Y-25 Z-26

Sample RSA Decryption

- How to compute d?
  - Recall: $ed \equiv 1 \pmod{\varphi(n)}$ (where $\varphi(n) = (p-1)(q-1)$)
  - So d is inverse of e mod $\varphi(n)$.
  - How to compute modular inverse?
    - Use extended Euclidean algorithm
    - … or Wolfram Alpha ☺
    - Note that this is hard if you don’t know $\varphi(n)$ (i.e., can’t factor n).

Public Key Crypto Summary

- Diffie-Hellman: Why is it secure?
  - Discrete log; computational DH problem; decisional DH problem are hard.
- RSA: Why is it secure?
  - Taking eth root is hard; Factoring is hard.

CRYPTOGRAPHY BACKDOORS

“Political and law enforcement leaders in the United States and the United Kingdom have **called for Internet systems to be redesigned to ensure government access to information** — even encrypted information. They argue that the growing use of encryption will neutralize their investigative capabilities. They propose that data storage and communications systems must be designed for exceptional access by law enforcement agencies."

Abelson, Harold, et al. "Keys under doormats: mandating insecurity by requiring government access to all data and communications." *Journal of Cybersecurity* 1.1 (2015): 69-79.

Some argue against ‘backdoors’ by saying:

“First, providing exceptional access to communications would **force a U-turn from the best practices** now being deployed to make the Internet more secure…

Second, building in exceptional access would substantially **increase system complexity**…

Third, exceptional access would create **concentrated targets** that could attract bad actors.”

Ibid

“We aren’t seeking a back-door approach**. We want to use the front door, with clarity and transparency, and with clear guidance provided by law.** We are completely comfortable with court orders and legal process — front doors that provide the evidence and information we need to investigate crime and prevent terrorist attacks.” -- James Comey

James B. Comey, “Going Dark: Are Technology, Privacy, and Pub- lic Safety on a Collision Course?” Oct. 2014, speech at the Brookings Institution. [Online]. Available: https://www.fbi.gov/news/speeches/ going-dark-are-technology-privacy-and-public-safety-on-a-collision-course