Lecture 20: RSA cryptography

- Algorithm overview
- A few computational details
- Why is it secure?
Shared (secret) key crypto

Sender
secret
msg → Enc

Attacker (network)
cyphertext

Recp
secret
Dec → msg.

Public key crypto

Sender
msg
public key
Enc

cypher

public key
Dec

private key: only known to Recipient.

Analogy: like an array of comment boxes. Private key opens an individual box; public key identifies where the box is.
RSA cryptosystem

Sender

pub key: m, k

msg

C := [msg]^k

ciphertext: c = [msg]^k

Recipient

k^{17} = 5

C = \sqrt[k]{17} = \sqrt[17]{5}

take k-th root of C

k^{17}C

\nu

C

\circ

not well defined

by defn, same
- for \([k]^{-1}\) to exist, \([k]_{\phi(m)}\) must be a unit

- choosing a unit:
  - pick a prime \(p\) (e.g. \(p = 7\)).
  - check whether \(k\) is a unit \(mod\) \(p\).
    - if not: try again with \(p\).
  - Note: almost everything is a unit if \(m\) is large.

- finding \([k]^{-1}\):
  - find \(s\) with \(1 = sk + t\phi(m) \in \mathbb{Z}\).
  - then \([k]^{-1}_{\phi(m)} = [s]_{\phi(m)}\).
Q: Are there enough primes?
A: Yes. (proof beyond scope of the course)

How do I find large primes?
A: There are efficient probabilistic algorithms for testing primality. (proof beyond scope of the course)
Fast exponentiation

want to find $a^b$ for large $b$

\[
\left[ 5^{14} \right] = \left[ 5^{8+4+2} \right] = \left[ 5^8 \cdot 5^4 \cdot 5^2 \right]
\]

write 14 as sum of powers of 2.

\((1110)_2 = 14 = 8 + 4 + 2\)

\[1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0\]

\[\text{(mod 7)}\]

1. $5^2 = 25$
2. $5^4 = 625$
3. $5^8 = (625)^2$
4. 2 more: $5^8 \cdot 5^4 \cdot 5^2$

\[
\begin{align*}
[5^2] &= 4 \\
\end{align*}
\]