15-251: Great Theoretical Ideas In Computer Science

Recitation 11

Announcements

- We have a midterm next Wednesday (November 18).

Number theory warm-up

(a) Why is $\mathbb{Z}_n^*$ closed under multiplication? (Prove that $x, y \in \mathbb{Z}_n^* \implies xy \in \mathbb{Z}_n^*$.)

(b) Prove that for any two distinct primes p, q, we have $\phi(pq) = (p-1)(q-1)$. (What about $\phi(p^2)$?)

Actual interesting stuff (part 1)

Understand Diffie-Hellman key exchange and be able to answer the questions below.

Alice		Bob
Picks a prime p	(1)	
Picks a generator $B \in \mathbb{Z}_P^*$	(2)	
Randomly draws $E_1 \in \mathbb{Z}_{\phi(P)}$	(3)	
Computes $B^{E_1} \in \mathbb{Z}_P^*$	(4)	
Sends $P, B \in \mathbb{Z}_P^*, B^{E_1} \in \mathbb{Z}_P^*$	(5)	Receives $P, B \in \mathbb{Z}_P^*, B^{E_1} \in \mathbb{Z}_P^*$
	(6)	Randomly draws $E_2 \in \mathbb{Z}_{\phi(P)}$
	(7)	Computes $B^{E_2} \in \mathbb{Z}_P^*$
	(8)	Sends $P, B \in \mathbb{Z}_P^*, B^{E_2} \in \mathbb{Z}_P^*$
Compute $(B^{E_2})^{E_1} = B^{E_1 E_2} \in \mathbb{Z}_P^*$	(9)	Compute $(B^{E_1})^{E_2} = B^{E_1 E_2}$

- In lines 3 and 5, where we pick random exponents, why are we picking from $\mathbb{Z}_{\phi(P)}$ rather than $\mathbb{Z}_P^*$ or $\mathbb{Z}$?
- Lines 4, 6, and 9 involve modular exponentiation. How can we accomplish this efficiently?
- What information do we assume an eavedropper wouldn't be able to derive? Why would it be bad if an eavesdropper could derive this information?
- In line 2, why do we need a generator? Why not any element?
- I thought cryptography was about sending messages. Why are Alice and Bob trying to secretly agree on an element of $\mathbb{Z}_P^*$?

Actual interesting stuff (part 2)

Understand RSA and be able to answer the questions below.

Alice		Bob
	(1)	Secretly chooses large primes P, Q
	(2)	Computes $N = PQ$ and chooses $E \in \mathbb{Z}^*_{\phi(N)}$
	(3)	Secretly computes $D = E^{-1} \in \mathbb{Z}^*_{\phi(N)}$
Prepares to encrypt message M	(4)	Publishes (N, E)
Computes $C = M^E \in \mathbb{Z}^*_N$	(5)	
Sends C	(6)	Receives C
	(7)	Computes $C^D = (M^E)^D = M^{ED} = M^{EE^{-1}} = M$

- Why are E, D chosen from $\mathbb{Z}^*_{\phi(N)}$ rather than $\mathbb{Z}_{\phi(N)}$?
- How does Bob efficiently invert E in line 3?
- Why doesn't Bob just pick a random big number N?
- What would happen if Bob published P, Q too?
- In what ways could an eavesdropper attempt to crack the encryption? Why is it hard to do so?