15-251: Great Theoretical Ideas In Computer Science

Recitation 14

Lecture Review

- **Multiplicative set of integers modulo** N: $\mathbb{Z}_N^* = \{A \in \mathbb{Z}_N : \gcd(A, N) = 1\}$
- **Totient function**: Euler's totient function, denoted $\phi(N)$, is the number of integers in the set $\mathbb{Z}_N$ that are relatively prime to N. $\phi(N) = |\mathbb{Z}_N^*|$.
- **Fast modular exponentiation**: To compute $A^E \bmod N$, repeatedly square A, always mod N. Multiply together the powers of A corresponding to the binary digits of E, again, always mod N.

Diffie Hellman

Recall the Diffie-Hellman protocol for securely generating a secret key over a public communication channel:

Apoorva		Bhagwat
Picks a large 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, B^{E_1}	(5)	Receives P, B, B^{E_1}
	(6)	Randomly draws $E_2 \in \mathbb{Z}_{\phi(P)}$
	(7)	Computes $B^{E_2} \in \mathbb{Z}_P^*$
Receives B^{E_2}	(8)	Sends B^{E_2}
Computes $(B^{E_2})^{E_1} = B^{E_1 E_2} \in \mathbb{Z}_P^*$	(9)	Computes $(B^{E_1})^{E_2} = B^{E_1 E_2} \in \mathbb{Z}_P^*$

- In line 2, why must B be a generator?
- In lines 3 and 5, why are the random exponents chosen from the set $\mathbb{Z}_{\phi(P)}$?
- Lines 4, 6, and 9 involve modular exponentiation. How can we accomplish this efficiently?
- An eavesdropper can obtain $B, B^{E_1}, B^{E_2} \in \mathbb{Z}_P^*$. Can she efficiently recover $B^{E_1 E_2}$?
- Why is this protocol useful?

Does it break?

Assume we have the RSA problem with (E, N) being the public key and (D, N) the private key, where D is a renaming of E^{-1} from lecture. Further assume $N = PQ$ where P and Q are odd primes with $P < Q$. We will denote a message by M and the ciphertext by $C = M^E \bmod N$. Determine if the information given is enough to crack RSA efficiently.

(a) You are given $\phi(N)$ and the public key.

(b) You are given $Q^{-1} \bmod P$, $P^{-1} \bmod Q$ and the public key.

(c) You are given Q, $P^{-1} \bmod Q$ and E.

(d) You are given P, Q, $D \bmod (P-1)$ and $D \bmod (Q-1)$ (no public key).

ElGamal

The ElGamal encryption system is a way of using the Diffie-Hellman protcol to exchange encrypted messages. Suppose Apoorva wants to send a message M to Bhagwat.

Apoorva		Bhagwat
	(1)	Picks a large prime P
	(2)	Picks a generator $B \in \mathbb{Z}_P^*$
	(3)	Randomly draws $E_1 \in \mathbb{Z}_{\phi(P)}$
	(4)	Computes $B^{E_1} \in \mathbb{Z}_P^*$
Receives P, B, B^{E_1}	(5)	Sends P, B, B^{E_1}
Randomly draws $E_2 \in \mathbb{Z}_{\phi(P)}$	(6)	
Encode M as an element of $\mathbb{Z}_P^*$	(7)	
Computes $B^{E_2}, MB^{E_1E_2} \in \mathbb{Z}_P^*$	(8)	
Sends $(B^{E_2}, MB^{E_1E_2})$	(9)	Receives $(B^{E_2}, MB^{E_1E_2})$
	(10)	Computes $(B^{E_2})^{E_1} = B^{E_1E_2} \in \mathbb{Z}_P^*$
	(11)	Computes $(B^{E_1E_2})^{-1} \in \mathbb{Z}_P^*$
	(12)	Computes $(MB^{E_1E_2})(B^{E_1E_2})^{-1} = M \in \mathbb{Z}_P^*$

Suppose $P = 17$, $B = 3$. Bhagwat sends Apoorva $(17, 3, 6)$ (line 5) (Note: $6 = 3^{15}$). Apoorva sends back $(7, 1)$ (line 9). What is the decrypted message?