Diffie-Hellman Key Exchange

1. Alice and Bob share prime p and generator g
2. Alice sends g^a mod p to Bob; a:1<a<p-1 is secret
3. Bob sends g^b mod p to Alice; b:1<b<p-1 is secret
4. Alice computes the shared key $k=(g^b)^a \pmod{p}$
5. Bob computes the shared key $k=(g^a)^b \pmod{p}$

Diffie-Hellman Key Exchange (example)

1. p=227, generator g=2
2. Alice selects a secret key a

   a must range from 1 to 226

   a=51

   $g^a=2^{51}=96 \pmod{227}$

   Alice sends 96 to Bob

Diffie-Hellman Key Exchange (example)

2. Bob selects a secret key b

   b must range from 1 to 226

   b=92

   $g^b = 2^{92} = 9 \pmod{227}$

   Bob sends 9 to Alice

Diffie-Hellman Key Exchange (example)

4. Alice computes

   $k = 9^{51} = 167 \pmod{227}$

5. Bob computes

   $k = 96^{92} = 167 \pmod{227}$

Diffie-Hellman Key Exchange (exercise)

prime p=227, generator g=2

a=25

b=157

k-? , g^a, g^b -?

Diffie-Hellman Key Exchange (exercise)

1. p=227, generator g=2
2. a=25

   $g^a=2^{25}=200 \pmod{227}$
3. b=157

   $g^b=2^{157}=56 \pmod{227}$

Diffie-Hellman Key Exchange (exercise)

4. Alice computes
   $k = 56^{25} = 98 \pmod{227}$
5. Bob computes
   $k = 200^{157} = 98 \pmod{227}$

Finding generators

1. Factor $p-1$: $p-1 = q_1^{k_1} q_2^{k_2} \cdot \ldots \cdot q_m^{k_m}$
2. Select $g: 1 < g < p-1$
3. For each factor q_i compute $g^{\frac{p-1}{q_i}}$ mod p. If equals to 1 then g is not a generator, go to Step 2. Otherwise, g is a generator.

Finding generators (example)

$p = 307,\ p - 1 = 306 = 2^1 3^2 17^1$

Try $g = 2$:

$2^{\frac{306}{2}} \bmod 307 = 2^{153} \bmod 307 = 306$

$2^{\frac{306}{17}} \bmod 307 = 2^{18} \bmod 307 = 273$

$2^{\frac{306}{3}} \bmod 307 = 2^{102} \bmod 307 = 1$

=> 2 is not a generator for 307

Finding generators (example)

$p = 307,\ p - 1 = 306 = 2^1 3^2 17^1$

Try $g = 5$:

$5^{\frac{306}{2}} \bmod 307 = 5^{153} \bmod 307 = 306$

$5^{\frac{306}{17}} \bmod 307 = 5^{18} \bmod 307 = 81$

$5^{\frac{306}{3}} \bmod 307 = 5^{102} \bmod 307 = 289$

=> 5 is a generator for 307