CS566 Fall, 2015

Homework Assignment #7
Student: Shuo Yang
GradeID: 50

---

1. What are some of the benefits of using Diffie-Hellman over RSA for key exchange?

   First of all, Diffie-Hellman has performance advantage over RSA because generating DH keys is cheap, while generating RSA keys is expensive. Second, DH allows two people who dont know each other to securely exchange symmetric keys. RSA requires that they know each others public keys. Third, DH is often used for (Perfect) Forward Secrecy (PFS) since DH key generation is cheap.

2. What is the things RSA can be used to perform whereas Diffie-Hellman cannot?

   RSA can be used for encryption and decryption while DH is just a key exchange algorithm. In addition, RSA can also be used for digital signatures.

3. What is forward secrecy?

   A communication protocol has forward secrecy if the compromise of long-term keys does not compromise past session keys.

4. Let p = 29. Let g = 5. Let Alices secret x = 7. Let Bobs secret y = 17. Compute K1. Compute K2. Show your work.

   Alice:
   $X = g^x \mod p = 5^7 \mod 29 = 28$

   Bob:
   $Y = g^y \mod p = 5^{17} \mod 29 = 9$

   Alice:
   $K_1 = Y^x \mod p = 9^7 \mod 29 = 28$

   Bob:
   $K_2 = X^y \mod p = 28^{17} \mod 29 = 28$

5. Compute $\phi(1343)$. Show your work.

   First, identify the prime factors of 1343: $1343 = 17*79$. Therefore $\phi(1343) = (17-1)*(79-1) = 1248$.

6. Compute $3232313123213^{24} \mod 35$. Show your work.

   Since $35 = 5 * 7$, $\phi(35) = 4 * 6 = 24$.
   And 3232313123213 is relatively prime to 35 since $GCD(3232313123213, 35) = 1$ because none of $5, 7$ or 35 is a factor of 3232313123213.
   According to Euler's theorem, $3232313123213^{24} \mod 35 = 3232313123213^{\phi(35)} \mod 35 = 1$.

7. Compute $822981828882^{264} \mod 299$. Show your work.

   Since $299 = 13 * 23$, its prime factors are 13 and 23. Therefore $\phi(299) = 12 * 22 = 264$.
   And 822981828882 is relatively prime to 299 since $GCD(822981828882, 299) = 1$ because none of

$13, 23$ or 299 is a factor of 822981828882.
According to Euler's theorem, $822981828882^{264} \mod 299 = 822981828882^{\phi(299)} \mod 299 = 1$.