CS236 HW8 – Teng Xu

1) (2 pts) Compute the modular exponentiation: $c \equiv b^e \pmod m$ for $b = 4$, $e = 13$, and $m = 497$, via binary method described at slide 15 of Lecture 8.

1. $b=4 \quad e=13 \quad m=497$

$e = a_0 \cdot 2^0 + a_1 \cdot 2^1 + a_2 \cdot 2^2 + a_3 \cdot 2^3$

$= 1 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3 = 13$

$c \equiv \prod_{i=0}^{n-1} (b^{2^i})^{a_i} \pmod m \equiv 4^1 \cdot 4^4 \cdot 4^8 \pmod{497}$

$c = 445$

2) (10 pts) Calculate Euler's totient function Φ(n) (defined at Lecture 9) for the following n:

2. a. $\phi(5) = 5-1 = 4$

b. $\phi(7) = 7-1 = 6$

c. $\phi(9) = \phi(3^2) = 3^2 - 3^1 = 6$

d. $\phi(10) = \phi(5 \cdot 2) = (5-1)(2-1) = 4$

e. $\phi(11) = 11-1 = 10$

f. $\phi(13) = 13-1 = 12$ $<$ $\phi(35) = \phi(5 \cdot 7) = 4 \cdot 6 = 24$

g. $\phi(131) = 131-1 = 130$

h. $\phi(143) = \phi(13 \cdot 11) = (12)\cdot(10) = 120$

i. $\phi(2537) = \phi(43 \cdot 59) = 42 \cdot 58 = 2436$

$\phi(p) = p-1$

$\phi(p^k) = p^k - p^{k-1}$

$\phi(p \cdot q) = \phi(p) \cdot \phi(q)$, $\gcd(p,q)=1$

3) (5 pts) Use Fermat's little theorem, Euler theorem (see Lecture 9), Python function computing multiplicative inverse (written for a previous homework), and math formulas for decrypting RSA encryption (at slide 13 of Lecture 9) to calculate the following:

3. a. $123456789^{131} \bmod 131 = 123456789 \bmod 131 = 31$

$a^p \equiv a \pmod p$ when p is a prime

b. $123456789^{131} \equiv 123456789^{130} \cdot 123456789 \pmod{131} = 31$

$\therefore 123456789^{130} \pmod{131} \cdot 31 = 31$

$\therefore 123456789^{130} \bmod 131 = 1$

c. $123456789^{\phi(143)} \bmod 143 = 1$

$\gcd(143, 123456789) = 1$

because $m^{\phi(n)} \equiv 1 \pmod n$

d. $\phi(2537) = \phi(43 \cdot 59) = 42 \cdot 58 = 2436$

multiplicative inverse of 13 mod 2436 is 937 using the python function

$\phi(p \cdot q) = \phi(p) \cdot \phi(q)$

e. use RSA Encryption and Decryption

$\phi(2537) = \phi(43 \cdot 59) = 42 \cdot 58 = 2436$

multiplicative inverse of 13, 2436 is 937

so that $(1415^{13} \bmod 2537)^{937} \bmod 2537 = 1415$

It is the same message after encryption and decryption.

4) (2 pts) What is the original message encrypted using the RSA system with n =43·59 and e =13 if the encrypted message is 0667 1947 0671?

4. $n = 43 \cdot 59$ $e = 13$ $\gcd(13, 43 \cdot 59) = 1$

$d = 937$

0667 1947 0671

$0667^{937} \bmod 2537 = 1808$ 1808 1121 0417

$1947^{937} \bmod 2537 = 1121$ S I L V E R

$0671^{937} \bmod 2537 = 0417$

5) (2 pts) Encrypt the message UPLOAD using the RSA system with n =3233 and e =17.

5. UPLOAD $n = 3233$ $e = 17$

2015 1114 0003

$2015^{17} \bmod 3233 = 2545$ 2545 2757 1211

$1114^{17} \bmod 3233 = 2757$

$0003^{17} \bmod 3233 = 1211$

6) (2 pts) Decrypt the encrypted message, obtained in the previous problem, showing all the steps of RSA decryption, using the factorization: n=53·61.

6. $\phi(3233) = \phi(53 \cdot 61) = \cancel{53}\ 52 \cdot 60 = 3120$ $\quad gcd(17, 3120) = 1$

$d = 2753$ multiplicative inverse of $(17, 3120) = 2753$

$2545^{2753} \bmod 3233 = 2015$

$2757^{2753} \bmod 3233 = 1114$ $\quad$ 2015 1114 0003

$1211^{2753} \bmod 3233 = 0003$