Introduction to Cryptography: Homework #5

Due on June 23, 2019 at 11:59pm

Professor Manuel

ShiHan Chan

Problem 1

Part One

Since the decryption step of RSA needs to use Euler's thereom, and the requirement of it is that m, n are coprime.

$ed \equiv 1 \mod \varphi(n)$

$c^d \equiv m^{ed} \equiv m^{ed \mod \varphi(n)} \equiv m \mod n$

Part Two

Assume $k = t\varphi(n)$, t is a positive integer

(a)

$m^k \equiv (m^{\varphi(n)})^t \equiv 1^t \equiv 1 \mod n$(Euler theorem)

Since n=pq, $m^k \equiv 1 \mod p$ and $m^k \equiv 1 \mod q$.

(b)

If gcd(m,n)=1, according to (a), $m^{k+1} \equiv m \mod p$ and $m^{k+1} \equiv m \mod q$.

If gcd(m,n)=p, suppose a is the integer such that gcd($\frac{m}{p^a}$,q)=1, $m^{k+1} \equiv (p^a)^{k+1}(\frac{m}{p^a})^{k+1} \equiv p^a \frac{m}{p^a} \equiv m \mod n$, so $m^{k+1} \equiv m \mod p$ and $m^{k+1} \equiv m \mod q$.

If gcd(m,n)=q, the result is same as previous step.

Part Three

(a)

$ed \equiv 1 \mod \varphi(n)$

, so $ed - \varphi(n) * t = 1$, t is an integer, $ed = k + 1$, then according to 2(b) we can get $m^{ed} \equiv m \mod n$ for any m.

(b)

It's not necessary to have gcd(m,n)=1 since we can still decrypt the plaintext m from ciphertext c through $c^d \equiv m^{ed} \equiv m \mod n$ for any m.

Problem 2

$n = pq = 11413 = 101 * 113$
$\varphi(n) = \varphi(p) * \varphi(q) = 100 * 112 = 11200$
$ed \equiv 1 \mod \varphi(n)$
$7467 * d \equiv 1 \mod 11200$
Apply the extended euclidean algorithm, we can get d=3
$m \equiv c^d \mod n$
$m \equiv 5859^3 \mod 11413$
Apply the modulo exponentiation, we can get:
$m \equiv 1415 \mod 11413$

Problem 3

1.
e is encryption key and d is decryption key, if they are both small, the encryption and decryption speed will be faster by modulo exponentiation.
$c \equiv m^e \mod n$
$m \equiv c^d \mod n$
2. 4.
Suppose n is given (n=pq)and we want to find two primes p and q, e is public encryption key , then we can find e,q in this way:
We find the approximation of $\frac{e}{n}$ recursively by extended eudlidean algorithm, and the calculation process is listed below:
$\frac{77537081}{317940011} = 0 + \frac{1}{4+a_1}$
$a_1 = \frac{1}{9+a_2}$
$a_2 = \frac{1}{1+a_3}$
$a_3 = \frac{1}{19+a_4}$
$a_4 = \frac{1}{1+a_5}$
$a_5 = \frac{1}{1+a_6}$
$a_6 = \frac{15}{9+a_7}$
$a_7 = \frac{3}{9+a_8}$
$a_8 = \frac{2}{9+a_9}$
$a_9 = \frac{3}{9+a_{10}}$
$a_{10} = \frac{1}{71+a_{11}}$
$a_{11} = \frac{1}{3+a_{12}}$
$a_{12} = \frac{1}{2}$
These fractions $\frac{a}{b} = \frac{1}{4}, \frac{9}{37}, \frac{10}{41}, \frac{199}{816} \cdots\cdots \frac{77537081}{317940011}$ becomes closer and closer to real $\frac{e}{n}$.
For each fraction in the series, we calculate $\varphi(n) = \frac{eb-1}{a}$, then solve quadratic equation:
$x^2 - (n - \varphi(n) + 1)x + n = 0$
If the solutions are not integers, we try the next fraction in the series, until we find all solutions are integers. In problem 4, we try the first element in the series, and we find $x_1 = 7791848.2$,$x_2 = 40.81$, and we try the second fraction. Second fraction we find coefficient of x is -823543.1111, so the solutions will not be integers, too. For third fraction, we find $x_1 = 12457, x_2 = 25523$, and we can find n=12457*25523=317940011.

3.
According to Wienner's theorem, the decryption key must be bigger than $\frac{1}{3}n^{\frac{1}{4}}$, and the key must be radomly selected from safe range.

Problem 4

programming problem, done with second problem

Problem 5

1.
By calculating $c * 2^e \mod n$, and it equals to $2m \mod n$. n is odd. If 2m mod n is odd, $m = \frac{n+2m \mod n}{2}$. If 2m mod n is even $m = \frac{2m \mod n}{2}$.
2.

Problem 5 continued on next page...

No, double encryption wouldn't add any security. The RSA problem is factorization problem with n. If the attacker knows how to factorize n, the decryption method is same and the number of exponent doesn't matter.

3.

$4 * 516107^2 \equiv 187722^2 \mod 642401$

$(2 * 516107 + 187722)(2 * 516108 - 187722) \equiv 0 \mod 642401$

$1219936 * 844492 \equiv 0 \mod 642401$

4.

If there are three primes: p,q,r, then $\varphi(n) = \varphi(p) * \varphi(q) * \varphi(r) = (p-1)(q-1)(r-1)$

The decryption process and encryption process are same as two primes.

$ed \equiv 1 \mod \varphi(n)$

$c \equiv m^e \mod n$

$c^d \equiv m^{ed} \equiv m^{ed \mod \varphi(n)} \equiv m \mod n$

The only drawback is if we use three prime factors instead of two with same bit length n, then the length of each factor is shorter, and the factorization problem can be done more efficient, and the security is worse.

5.

97-1=96=$2^5 * 3$

Suppose the smallest generator is α, α must satisfy:

$\alpha^{48} \not\equiv 1 \mod 97$ and $\alpha^{32} \not\equiv 1 \mod 97$

Since 16 is common factor of 48 and 32, $\alpha^{16} \not\equiv \pm 1, 35, 61 \mod 97$

, $2^{16} \equiv 61 \mod 97$

$3^{16} \equiv 61 \mod 97$

$4^{16} \equiv 1 \mod 97$

$5^{16} \equiv 36 \mod 97$

Then 5 is the smallest generator of $U(Z/97Z)$.

6.

(a)

101-1=100=$2^2 * 5^2$

$2^{50} \equiv (2^{10})^5 \equiv 14^5 \equiv 100 \mod 101$

$2^{20} \equiv (2^{10})^2 \equiv 14^2 \equiv 95 \mod 101$

So 2 is a generator of G since $2^{50} \not\equiv 1 \mod 101$ and $2^{20} \not\equiv 1 \mod 101$.

(b)

$\log_2 24 = 3 * log_2 2 + log_2 3 = 3 + 69 = 72 (log_2 2 = 1)$

(c)

$\log_2 24 = log_2 125 = 3 * log_2 5 = 3 * 24 = 72$

7.

8.

(a)

$6^5 \equiv 10 \mod 11$, $6^5 = 10$ in $Z/11Z$

(b)

11-1=10=2*5

$2^5 \equiv 10 \mod 11$ and $2^2 \equiv 4 \mod 11$

2 is a generator of $U(Z/11Z)$ since $2^5 \not\equiv 1 \mod 11$ and $2^2 \not\equiv 1 \mod 11$

(c)

$2^x \equiv 6 \mod 11$

$(2^x)^5 \equiv 6^5 \mod 11$

$(-1)^x \equiv 10 \equiv -1 \mod 11$

So x is an odd integer.

Problem 6

1.
$3^x \equiv 2 \mod 65537$
$3^{16x} \equiv -1 \mod 65537$
$3^{32x} \equiv 1 \mod 65537$
$3^{65536} \equiv 1 \mod 65537$(since 3 and 65537 are coprime integers)
$65536|32x$ and $65536 \not| 16x$
$2048|x$ and $4096 \not| x$
2.
Consider the restriction in previous part, we know that x=2048(2k+1), where k=0,1,.....15, so there are 16 possible choices in total. And we apply modulo exponentiation to calculate and get $3^{2048} \equiv -8 \mod 65537$ and $3^{2048*31} \equiv 8192 \mod 65537$ and $3^{2048*27} \equiv 2 \mod 65537$
Then x=2048*27=55296
3.
From part 1, we know that $2048|x$ and $4096 \not| x$, so we assume that $x = 2^{11} + a*2^{12} + b*2^{13} + c*2^{14} + d*2^{15}$
Then apple Pohlig-Hellman algorithm to solve x For a, $\frac{3^x}{3^{2^{11}}}^{2^{15-12}} \equiv (2^{14})^8 \equiv -1 \mod 65537$, so a=1, we can calculate b=0,c=1,d=1 in the same method. So $x = 2^{11} + 2^{12} + 2^{14} + 2^{15} = 55296$
4.
$65537=2^{16}+1$ is in the form p^k+1, Suppose we have $p \equiv c^x \mod p^k+1$, we can find the generator of prime to find x. Because $p^{2k} \equiv c^{2k} \equiv 1 \mod p^k+1$, $\frac{p^k}{k} \not| x$ and $\frac{p^k}{2k}|x$. So there are k possible choices for x, and the decryption process is very easy. That explains why primes are not fitting a cryptographic context.