Chapter 10

10/10

12\. a. $n = 221$, $e = 5$ $d = e^{-1} \bmod \phi(n)$

$\phi(221) = \phi(13 \times 17) = 12 \times 16 = 192$ $d = 5^{-1} \bmod 192$

$= 77$

$192 = 38 \times 5 + 2$, $5 = 2 \times 2 + 1$ $2 = 2 \times 1 + 0$, $1 = 5 - 2 \times 2$

$2 = 192 - 38 \times 5 \rightarrow 1 = 5 - 2(192 - 38 \times 5) = 77 \times 5 - 2 \times 192$

b. $n = 3937$, $e = 17$

$\phi(3937) = \phi(31 \times 127) = 30 \times 126 = 3780$ $d = 17^{-1} \bmod 3780$

$= 3113$

$3780 = 222 \times 17 + 6$ $17 = 2 \times 6 + 5$

$6 = 1 \times 5 + 1$ $5 = 5 \times 1 + 0$ $1 = 6 - 1 \times 5$

$5 = 17 - 2 \times 6 \rightarrow 1 = 6 - 1 \times (17 - 2 \times 6) = 3 \times 6 - 1 \times 17$

$6 = 3780 - 222 \times 17 \rightarrow 1 = 3 \times (3780 - 222 \times 17) - 1 \times 17$

$= 3 \times 3780 - 667 \times 17$

$-667 \equiv 3113 \bmod 3780$

c. $p = 17$, $q = 23$ $e = 3$ find n, $\phi(n)$, d

$n = pq = 19 \times 23 = 437$

$\phi(n) = \phi(437) = 18 \times 22 = 396$

we can not find d. Because $\gcd(396, 3) \neq 1$

13\. $e = 17$, $n = 187 = 17 \times 11$

$\phi(n) = \phi(187) = 16 \times 10 = 160$ $d = e^{-1} \bmod \phi(n)$

$d = 17^{-1} \bmod 160 = 113$

In RSA, n must be set very large to make factorization difficult to keep the secret key d safe. If n is small and factorization is possible, an attacker can factor n to obtain d.

$160 = 9 \times 17 + 7$ $17 = 2 \times 7 + 3$

$7 = 2 \times 3 + 1$ $3 = 3 \times 1 + 0$ $1 = 7 - 2 \times 3$

$3 = 17 - 2 \times 7 \rightarrow 1 = 7 - 2 \times (17 - 2 \times 7) = 5 \times 7 - 2 \times 17$

$7 = 160 - 9 \times 17 \rightarrow 1 = 5 \times (160 - 9 \times 17) - 2 \times 17$

$= 5 \times 160 - 47 \times 17$

$-47 \equiv 113 \bmod 160$

14\. In RSA, given n, $\phi(n)$, calculate p, q

$pq = n \Rightarrow q = \frac{n}{p}$

$(p-1)(q-1) = \phi(n) \Rightarrow (p-1)(\frac{n}{p} - 1) = \phi(n) \Rightarrow (p-1)(\frac{n-p}{p}) = \phi(n)$

$\frac{(p-1)(n-p)}{p} = \phi(n) \Rightarrow (p-1)(n-p) = \phi(n) \cdot p \Rightarrow -p^2 + (n+1)p - n = \phi(n) \cdot p$

$p^2 - (n - \phi(n) + 1)p + n = 0$ solved by Quadratic formula.

$$p = \frac{n - \phi(n) + 1 + \sqrt{(n - \phi(n) + 1)^2 - 4n}}{2} \qquad q = \frac{n - \phi(n) + 1 - \sqrt{(n - \phi(n) + 1)^2 - 4n}}{2}$$

15\. Encryption is performed using $c = m^e \bmod n$, and decryption is performed using $m = c^d \bmod n$. Here, n must be the product of two prime numbers, p and q. If n is not a product of two primes, we cannot correctly calculate the value of $\phi(n)$, which means we cannot calculate the correct value of d. In the problem, since $n = 100$, and cannot be expressed as a product of two primes, encryption is possible, but decryption is feasible due to an incorrect value of d. Therefore, this problem has no solution.

19. Alice $P=8$ $\xrightarrow{\text{public key } (e=7,\ n=143)}$ $C=57$ Bob

Eve get $C=57$

Eve chosen-ciphertext attack

$n=11\times13$. $\phi(n)=10\times12=120$

$d=7^{-1} \bmod 120$

$120=17\times7+1$ $1=120-17\times7$

$d=-17 \bmod 120=103$

Eve can choose X in Z_n^* $X=3$ in Z_{143}^*

$Y=C\times X^e \bmod n \Rightarrow Y=57\times3^7 \bmod 143=106$

Eve send Y to Bob and asks him to decrypt it.

$Z=Y^d \bmod n=106^{103} \bmod 143=24$ Eve can get $Z=24$

So calculate $P=Z\times X^{-1} \bmod n = 24\times3^{-1} \bmod 143 = 24\times48 \bmod 143=8$

So Eve can get plaintext $P=8$

RSA is very vulnable to chosen-ciphertext attack

22. $P=47$. $q=11$. $n=pq=517$

In Rabin cryptosystem, $e=2$ and $d=\frac{1}{2}$. So $C\equiv P^2 (\bmod n)$ and $P\equiv C^{1/2} (\bmod n)$

a. $C=P^2 \bmod 517=17^2 \bmod 517=289$

b. Chinese remainder theorem

$a_1=+C^{(P+1)/4} \bmod p$ $a_2=-C^{(P+1)/4} \bmod p$

$b_1=+C^{(q+1)/4} \bmod q$ $b_2=-C^{(q+1)/4} \bmod q$

$a_1=289^{12} \bmod 47=17$ $a_2=-17$ $(17,5)$ $(17,-5)$ $(-17,5)$ $(-17,-5)$

$b_1=289^3 \bmod 11=5$ $b_2=-5$

$P_1\equiv17 \bmod 47$ $P_1\equiv5 \bmod 11$ $P_1=346$

$P_2\equiv17 \bmod 47$ $P_2\equiv-5 \bmod 11$ $P_2=17$ 17 is possible

$P_3\equiv-17 \bmod 47$ $P_3\equiv5 \bmod 11$ $P_3=500$

$P_4\equiv-17 \bmod 47$ $P_4\equiv-5 \bmod 11$ $P_4=171$

24. In ElGamal, $P=C_2(C_1^d)^{-1} \bmod p$

For example, If $(e_1,e_2,p)=(2,13,23)$, $d=5$, $m=15$,

$C_1=2^3 \bmod 23=8$, $C_2=15\times13^3 \bmod 23=17$ $(C_1,C_2)=(8,17)$

$\leftarrow C_2\times(C_1^d)^{-1}\neq C_1\times(C_2^d)^{-1}$

If C_1 and C_2 are not swapped, $P=17\times(8^5)^{-1} \bmod 23=17\times9^{-1} \bmod 23=17\times18 \bmod 23=15$

If C_1 and C_2 are swapped, $P=8\times(17^5)^{-1} \bmod 23=8\times12^{-1} \bmod 23=8\times2 \bmod 23=16$

As a result, the decrypted plaintext is $m=16$, which is different from the original plaintext $m=15$

In ElGamal encryption, If C_1 and C_2 are swapped, the receiver cannot correctly decrypt the message

25. $e_1=2$, $e_2=8$, $P=17$, $P'=37$, $r=9$

If Alice uses the same random exponent r to encrypt two plaintext P and P',
then if Eve discovers one of them, she can also find out the other.

$C_2 = P \times (e_2^r) \bmod p$, $C_2' = P' \times (e_2^r) \bmod p$.

$e^r = C_2 \times P^{-1} \bmod r$.

$P' = C_2' \times (e_2^r)^{-1} \bmod p = C_2' \times (C_2 \times P^{-1})^{-1} \bmod p = C_2' \times C_2^{-1} \times P \bmod p$

We can choose p which is bigger than 17, 37. And $e_1=2$ must be chosen as a primitive root of p.
So $p=53$ corresponds to this

Alice encrypt a message 17, 37 using $r=9$

$C_2 = 17 \times 8^9 \bmod 53 = 19$ $\quad$ $C_2' = 37 \times 8^9 \bmod 53 = 32$

If Eve intercepts $C_2=19$, $C_2'=32$ and Eve know $P=17$, then

$P' = C_2' \times C_2^{-1} \times P \bmod p = 32 \times 19^{-1} \times 17 \bmod 53$

$= 32 \times 14 \times 17 \bmod 53 = 37$.

Eve can get $P'=37$ using known-plaintext attack