Fundamentals of Cryptography

Homework 4

Sepehr Ebadi 9933243

Question 1

1)

$$y = x^e \bmod n$$
$$x = y^d \bmod n$$

$$n = p * q = 7 * 13 = 91$$
$$\emptyset(n) = (p-1) * (q-1) = 6 * 12 = 72$$
$$e * d = 1 \bmod \emptyset(n)$$
$$5^6 = 1 \bmod 72 \rightarrow (5^6)^{11} * 5^5 \bmod 72 \rightarrow 5^5 \bmod 72 \rightarrow 29$$
$$d = 5 \rightarrow e = 29$$

$$Encryption:$$
$$y = x^e \bmod n = 9^{29} \bmod 91 = 65$$
$$Decryption:$$
$$x = y^d \bmod n = 65^5 \bmod 91 = 9$$

2)

$$y = x^e \bmod n$$
$$x = y^d \bmod n$$

$$n = p * q = 11 * 13 = 143$$
$$\emptyset(n) = (p-1) * (q-1) = 10 * 12 = 120$$
$$e * d = 1 \bmod \emptyset(n)$$
$$e = 7 \rightarrow d = 103$$

$$Encryption:$$
$$y = x^e \bmod n = 4^7 \bmod 143 = 87$$
$$Decryption:$$
$$x = y^d \bmod n = 87^{103} \bmod 143 = 4$$

Question 2

1)

$$5^{117}\ mod\ 113$$

$initial\ x = 1$	1	1
$x^2 = 10$	5^2	25
$x^2.x = x^3 = 11$	25.5	12
$(x^3)^2 = x^6 = 110$	12^2	11
$x^6.x = x^7 = 111$	11.5	55
$(x^7)^2 = x^{14} = 1110$	55^2	87
$(x^{14})^2 = x^{28} = 11100$	87^2	$-2 = 111$
$x^{28}.x = x^{29} = 11101$	-2.5	-10
$(x^{29})^2 = x^{58} = 111010$	$(-10)^2$	-3
$(x^{58})^2 = x^{116} = 1110100$	$(-3)^2$	9
$x^{116}.x = x^{117} = 1110101$	9 .5	45

$$5^{117}\ mod\ 113 = 45$$

2)

$$7^{202}\ mod\ 123$$

$initial\ x = 1$	1	1
$x^2 = 10$	7^2	49
$x^2.x = x^3 = 11$	49.7	-26
$(x^3)^2 = x^6 = 110$	$(-26)^2$	61
$(x^6)^2 = x^{12} = 1100$	61^2	31
$(x^{12})^2 = x^{24} = 11000$	31^2	-26
$x^{24}.x = x^{25} = 11001$	-26.7	64
$(x^{25})^2 = x^{50} = 110010$	$(64)^2$	37
$(x^{50})^2 = x^{100} = 1100100$	$(37)^2$	16
$x^{100}.x = x^{101} = 1100101$	16.7	-11
$(x^{101})^2 = x^{202} = 11001010$	$(-11)^2$	$-2 = 121$

$$7^{202}\ mod\ 123 = 121$$

Question 3

1)

$$\emptyset(n) = (p-1) * (q-1) = 42 * 18 = 756$$
$$\gcd(e, \emptyset(n)) = 1$$
$$\gcd(45,756) = ?$$
$$\gcd(61,756) = ?$$

1. $1 < e < \phi(n)$
2. $\gcd(e,\phi(n))=1$

$\gcd(45,756)$

$756=16\cdot45+36$

$45=1\cdot36+9$

$36=4\cdot9+0$

$\gcd(45,756) = 9 \neq 1$, 45 is **not valid**.

$\gcd(61,756)$

$756=12\cdot61+24$

$61=2\cdot24+13$

$24=1\cdot13+11$

$13=1\cdot11+2$

$11=5\cdot2+1$

$2=2\cdot1+0$

$\gcd(61,756) =1$, 61 is **valid**.

2)

inverse of 61 modulo $\phi(n)=756$:

$61d \equiv 1 \pmod{756}$:

$756=12\cdot61+24$

$61=2\cdot24+13$

$24=1\cdot13+11$

$13=1\cdot11+2$

$11=5\cdot2+1$

$2=2\cdot1+0$

$$1 = 11 - 5.2$$
$$2 = 13 - 1.11 \rightarrow 1 = 11 - 5.(13 - 1.11) = 6.11 - 5.13$$
$$11 = 24 - 1.13 \rightarrow 1 = 6.(24 - 1.13) - 5.13 = 6.24 - 11.13$$
$$13 = 61 - 2.24 \rightarrow 1 = 6.24 - 11.(61 - 2.24) = 28.24 - 11.61$$
$$24 = 756 - 12.61 \rightarrow 1 = 28.(756 - 12.61) - 11.61$$
$$1 = 28.756 - 347.61$$

$$d = -347\ mod\ 756 \rightarrow d = 409$$

private key: $k = (p, d, q) = (43,19,409)$

Question 4

$$n = p * q = 31 * 37 = 1147$$
$$\emptyset(n) = 30 * 36 = 1080$$
$$e.d \equiv 1\ mod\ 1080$$
$$e = 17 \rightarrow d = 953$$

$$dp = d\ mod\ (p - 1) = 953\ mod\ 30 = 23$$
$$dq = d\ mod\ (q - 1) = 953\ mod\ 36 = 17$$

$$yp = y^{dp} mod\ p = 2^{23}\ mod\ 31$$
$$23 = 10111$$
$$2^1 mod\ 31 = 2$$
$$2^2 mod\ 31 = 4$$
$$2^4 mod\ 31 = 16$$
$$2^8 mod\ 31 = 8$$

$$2^{16} mod\ 31 = 2$$
$$2^{23} mod\ 31 = 2 * 8 * 16 * 4 * 2\ mod\ 31 = 28$$

$$yq = y^{dq} mod\ q = 2^{17}\ mod\ 37$$
$$17 = 10001$$
$$2^{1} mod\ 37 = 2$$
$$2^{2} mod\ 37 = 4$$
$$2^{4} mod\ 37 = 16$$
$$2^{8} mod\ 37 = 34$$
$$2^{16} mod\ 37 = 9$$
$$2^{17}\ mod\ 37 = 9 * 2 = 18$$

$$N1 = q = 37$$
$$M1 = N1^{-1} \rightarrow 37.x = 1\ mod\ 31 \rightarrow M1 = 26$$
$$N2 = p = 31$$
$$M2 = N2^{-1} \rightarrow 31.x = 1\ mod\ 37 \rightarrow M2 = 6$$

$$y = N1 * M1 * yp + N2 * M2 * yq = 37 * 26 * 28 + 31 * 6 * 18\ mod\ 1147 = 65$$

Question 5

1)

توابع یک‌طرفه، توابع ریاضی هستند که محاسبه آن‌ها در یک جهت ساده است، اما معکوس کردن آن‌ها بدون اطلاعات اضافی بسیار دشوار است. امنیت رمزنگاری کلید عمومی بر اساس این توابع بنا شده است.

تابع f(x) یک تابع یک‌طرفه است اگر:

۱. با داشتن x، محاسبه f(x) ساده باشد.

۲. با داشتن f(x)، یافتن x(پیش‌تصویر) بدون اطلاعات خاص بسیار دشوار باشد.

این توابع به رمزنگاری کلید عمومی اجازه می‌دهند تا ارتباط امن را بدون نیاز به تبادل کلید از قبل ممکن کنند. و امنیت سیستم‌های رمزنگاری بر اساس همین ویژگی دشواری معکوس‌پذیری است.

مثال:

در الگوریتمRSA ، ضرب دو عدد اول p و q برای محاسبه n=p·q ساده است، اما یافتن pو q از n تجزیه n بسیار دشوار است.

کلید عمومی(n,e)

کلید خصوصی d :که به p و qوابسته است.

امنیت RSA به دلیل سختی تجزیه اعداد به عوامل اول تضمین می‌شود.

2)

مسئله لگاریتم گسسته شامل یافتن xدر معادله زیر است:

$$h = g^x \bmod p$$

پروتکل تبادل کلید دیفی-هلمن (Diffie-Hellman) : این پروتکل به دلیل سختی حل مسئله لگاریتم گسسته، به دو طرف اجازه می‌دهد یک کلید مشترک را بدون تبادل مستقیم آن تولید کنند.

رمزنگاری منحنی بیضوی (ECC): از مسئله لگاریتم گسسته روی منحنی‌های بیضوی استفاده می‌کند که نسبت به لگاریتم گسسته امنیت بیشتری برای اندازه کلید برابر فراهم می‌کند.

امنیت از دشواری حل معادله

$$h = g^x \bmod p$$

با p بزرگ ناشی می‌شود.

درECC ، حل مسئله لگاریتم گسسته روی منحنی‌های بیضوی سخت‌تر است و ECC امنیت بیشتری برای اندازه کلید مشابه فراهم می‌کند.

مسئله تجزیه اعداد صحیح شامل یافتن عوامل اول pو qیک عدد مرکب n است، به‌طوری‌که $n=p\cdot q$.

الگوریتم RSA : فرآیند رمزگذاری و رمزگشایی بر اساس سختی تجزیه عدد مرکب nبه عوامل اول آن است.

کلید عمومی(n,e) :

کلید خصوصی d :که از $\phi(n)=(p-1)(q-1)$ به دست می‌آید.

امنیت RSA بر پایه فرض دشواری تجزیه اعداد بزرگ به عوامل اول است.

استفاده از اندازه کلیدهای بزرگ‌تر (مانند ۲۰۴۸ یا ۴۰۹۶ بیت) احتمال موفقیت در حمله را به شدت کاهش می‌دهد.

Question 6

رویکرد کلی:

در این پیاده‌سازی، هدف تولید کلیدهای RSA شامل کلید عمومی (n,e)و کلید خصوصی d است. سپس، از این کلیدها می‌توان برای رمزنگاری و رمزگشایی پیام‌ها استفاده کرد. این فرآیند شامل مراحل زیر است:

۱. **تولید اعداد اول p و q**

دو عدد اول بزرگ pو qبه صورت تصادفی تولید می‌شوند. این اعداد مبنای ساخت سیستم رمزنگاری هستند و امنیت کل سیستم به انتخاب صحیح این اعداد بستگی دارد.

۲. **محاسبه n و $\phi(n)$**

n به صورت $p \times q$محاسبه می‌شود.

$\phi(n)$(تابع اویلر) به صورت $(p-1)\times(q-1)$ محاسبه می‌شود که در تعیین کلیدهای رمزنگاری نقش اساسی دارد.

۳. **انتخاب عدد e :**

عدد e باید شرط $\gcd(e,\phi(n))=1$ را برآورده کند، به این معنا که e نسبت به $\phi(n)$ اول باشد. این عدد به صورت تصادفی تولید می‌شود و در صورت عدم تطابق با شرط ذکر شده، تکرار می‌شود تا مقدار مناسبی پیدا شود.

٤. **محاسبه d :**

d معکوس ضربی e به پیمانه $\phi(n)$ است که با استفاده از الگوریتم اقلیدسی توسعه‌یافته محاسبه می‌شود. این عدد کلید خصوصی را تشکیل می‌دهد.

٥. **بازگشت کلیدها:**

کلید عمومی شامل (n,e) است که برای رمزنگاری استفاده می‌شود.

کلید خصوصی مقدار d است که برای رمزگشایی استفاده می‌شود.

٦. **تست اول بودن(Primality Test) :**

از تست میلر–رابین برای بررسی اول بودن اعداد pو qاستفاده شده است. این روش یک الگوریتم احتمالی کارآمد است که برای اعداد بزرگ قابل اعتماد است.

عکس خروجی کد:

```
PS E:\IUT\Lessons\Semester 9th\Cryptography Basic\HW\HW4> python -u "e:\IUT\Lessons\Semester 9th\Cryptography Basic\HW\HW4\Q6.py
Public Key: (409, 671)
Private Key: 289

Original Message: Sepehr Ebadi 9933243
Ciphertext: [321, 589, 105, 589, 372, 267, 32, 587, 516, 324, 45, 112, 32, 622, 622, 349, 349, 233, 271, 349]
Decrypted Message: Sepehr Ebadi 9933243
PS E:\IUT\Lessons\Semester 9th\Cryptography Basic\HW\HW4>
```

```
PS E:\IUT\Lessons\Semester 9th\Cryptography Basic\HW\HW4> python -u "e:\IUT\Lessons\Semester 9th\Cryptography Basic\HW\HW4\Q6.py"
Public Key: (7703, 13861)
Private Key: 6199

Original Message: HW4 Cryptography
Ciphertext: [6316, 13698, 6706, 4350, 8540, 100, 5459, 5543, 6088, 7215, 3878, 100, 4788, 5543, 3846, 5459]
Decrypted Message: HW4 Cryptography
PS E:\IUT\Lessons\Semester 9th\Cryptography Basic\HW\HW4>
```