Introduction to Cryptography: Homework 3

Alvin Lin

January 2018 - May 2018

Exercise 1

Find the value of the Euler totient function $\phi(n)$ for $n = 937, 938, 939, 940, 941, 942$. Show the details of computations.

- $\phi(937) = 936$

$$\begin{aligned} 937 &= 937^1 \\ \phi(937) &= (937^1 - 936^0) = (937 - 1) = 936 \end{aligned}$$

- $\phi(938) = 396$

$$\begin{aligned} 938 &= 2^1 \times 7^1 \times 67^1 \\ \phi(938) &= (2^1 - 2^0) \times (7^1 - 7^0) \times (67^1 - 67^0) \\ &= 1 \times 6 \times 66 = 396 \end{aligned}$$

- $\phi(939) = 624$

$$\begin{aligned} 939 &= 3 \times 313 \\ \phi(939) &= (3^1 - 3^0) \times (313^1 - 313^0) = 2 \times 312 = 624 \end{aligned}$$

- $\phi(940) = 368$

$$\begin{aligned} 940 &= 2^2 \times 5 \times 47 \\ \phi(940) &= (2^2 - 2^1) \times (5^1 - 5^0) \times (47^1 - 47^0) \\ &= 2 \times 4 \times 46 = 368 \end{aligned}$$

- $\phi(941) = 940$

$$\begin{aligned} 941 &= 941^1 \\ \phi(941) &= (941^1 - 941^0) = 940 \end{aligned}$$

- $\phi(942) =$

$$\begin{aligned} 942 &= 2 \times 3 \times 157 \\ \phi(942) &= (2^1 - 2^0) \times (3^1 - 3^0) \times (157^1 - 157^0) \\ &= 1 \times 2 \times 156 = 312 \end{aligned}$$

Exercise 2

Compute $41^{41} \mod 937$, using the modular square and multiply exponentiation algorithm. Show the details of the computation.

$$41 = 101001_2$$

Step	Accumulated Result	Binary Exponent
1	$r = 1^2 \times 41 \equiv 41 \mod 937$	1
2	$r = 41^2 \equiv 744 \mod 937$	10
3	$r = 744^2 \times 41 \equiv 836 \mod 937$	101
4	$r = 836^2 \equiv 831 \mod 937$	1010
5	$r = 831^2 \equiv 929 \mod 937$	10100
6	$r = 929^2 \times 41 \equiv 750 \mod 937$	101001

$$41^{41} \equiv 750 \mod 937$$

Exercise 3

Use the extended Euclidean algorithm to find the multiplicative inverse of 27 module n, if it exists, for $n = 1033, 1034, 1035$. Show the details of the computations.

- $27^{-1} \mod 1033 = 880$

$$\begin{aligned}
1033 &= 38 \times 27 + 7 \\
27 &= 3 \times 7 + 6 \\
7 &= 1 \times 6 + 1 \\
6 &= 6 \times 1 + 0 \\
gcd(1033, 27) &= 1 \\
1 &= 7 - 1 \times 6 \\
1 &= 7 - (27 - 3 \times 7) \\
&= -27 + 4 \times 7 \\
&= -27 + 4 \times (1033 - 38 \times 27) \\
&= -153 \times 27 + 4 \times 1033 \\
&= -153 \times 27 \mod 1033 \\
27^{-1} &= 880 \mod 1033
\end{aligned}$$

- $27^{-1} \mod 1034 = 383$

$$
\begin{aligned}
1034 &= 38 \times 27 + 8 \\
27 &= 3 \times 8 + 3 \\
8 &= 2 \times 3 + 2 \\
3 &= 1 \times 2 + 1 \\
gcd(1034, 27) &= 1 \\
1 &= 3 - 1 \times 2 \\
&= 3 - (8 - 2 \times 3) \\
&= -8 + 3 \times 3 \\
&= -8 + 3 \times (27 - 3 \times 8) \\
&= 3 \times 27 - 10 \times 8 \\
&= 3 \times 27 - 10 \times (1034 - 38 \times 27) \\
&= 383 \times 27 - 10 \times 1034 \\
&= 383 \times 27 \mod 1034 \\
27^{-1} &= 383 \mod 1034
\end{aligned}
$$

- $27^{-1} \mod 1035 =$

$$
\begin{aligned}
1035 &= 38 \times 27 + 9 \\
27 &= 3 \times 9 + 0
\end{aligned}
$$

No modular inverse exist for 27 modulo 1035.

Exercise 4

For each of the following compute the value of or argue that it is not defined. For at least two of the six cases below, do the computations without using any program, and describe briefly how you did it.

- discrete logarithm of 2 base 3 mod 11

$$
\begin{aligned}
&3^x \mod 11 \equiv 2 \\
&3^1 \mod 11 \equiv 3 \\
&3^2 \mod 11 \equiv 9 \mod 11 \equiv 9 \\
&3^3 \mod 11 \equiv 9 \times 3 \mod 11 \equiv 5 \\
&3^4 \mod 11 \equiv 5 \times 3 \mod 11 \equiv 4 \\
&3^5 \mod 11 \equiv 4 \times 3 \mod 11 \equiv 1 \\
&3^6 \mod 11 \equiv 1 \times 3 \mod 11 \equiv 3^1 \mod 11 \equiv 3
\end{aligned}
$$

We can calculate the discrete logarithm by brute force starting from an exponent of 1. This discrete logarithm is not defined since the modulo cycles and is not evenly distributed among all the numbers from 1 to 11.

- discrete logarithm of 3 base 2 mod 19

$$
\begin{aligned}
2^x &\mod 19 \equiv 3 \\
2^1 &\mod 19 \equiv 2 \quad \mod 19 \equiv 2 \\
2^2 &\mod 19 \equiv 2 \times 2 \quad \mod 19 \equiv 4 \\
2^3 &\mod 19 \equiv 4 \times 2 \quad \mod 19 \equiv 8 \\
2^4 &\mod 19 \equiv 8 \times 2 \quad \mod 19 \equiv 16 \\
2^5 &\mod 19 \equiv 16 \times 2 \quad \mod 19 \equiv 13 \\
2^6 &\mod 19 \equiv 13 \times 2 \quad \mod 19 \equiv 7 \\
2^7 &\mod 19 \equiv 7 \times 2 \quad \mod 19 \equiv 14 \\
2^8 &\mod 19 \equiv 14 \times 2 \quad \mod 19 \equiv 9 \\
2^9 &\mod 19 \equiv 9 \times 2 \quad \mod 19 \equiv 18 \\
2^{10} &\mod 19 \equiv 18 \times 2 \quad \mod 19 \equiv 17 \\
2^{11} &\mod 19 \equiv 17 \times 2 \quad \mod 19 \equiv 15 \\
2^{12} &\mod 19 \equiv 15 \times 2 \quad \mod 19 \equiv 11 \\
2^{13} &\mod 19 \equiv 11 \times 2 \quad \mod 19 \equiv 3 \\
& x = 13
\end{aligned}
$$

  The discrete logarithm of 3 base 2 mod 19 is 13. $2^{13} \mod 19 \equiv 3$.

- discrete logarithm of 3 base 3 mod 97

$$3^x \mod 97 \equiv 3 \quad x = 1$$

- discrete logarithm of 3 base 4 mod 97

$$4^x \mod 97 \equiv 3$$

  No discrete logarithm exists. The resulting modulus will enter a loop and will never be equal to 3.

- discrete logarithm of 4 base 3 mod 97

$$3^x \mod 97 \equiv 4 \quad x = 38$$

  See attached Python program for calculation script.

- discrete logarithm of 43 base 3 mod 97

$$3^x \mod 97 \equiv 43 \quad x = 22$$

  See attached Python program for calculation script.

Exercise 5

Solve problem 6.10 on page 171. Show the details of the computations. Compute the inverse $a^{-1} \mod n$ with Fermat's Theorem (if applicable) or Euler's Theorem:

- $a = 4, n = 7$

$$
\begin{aligned}
a^{-1} &= a^{p-2} \mod p \quad \text{if } p \text{ is prime} \\
4^{-1} &= 4^{7-2} \mod 7 \\
&= 4^5 \mod 7 = 2
\end{aligned}
$$

- $a = 5, n = 12$

$$\begin{aligned} 12 &= 2 \times 5 + 2 \\ 5 &= 2 \times 2 + 1 \\ gcd(12, 5) &= 1 \\ 1 &= 5 - (2 \times 2) \\ &= 5 - 2 \times (12 - 2 \times 5) \\ &= 5 \times 5 - 2 \times 12 \\ &= 5 \times 5 \mod 12 \\ 5^{-1} &= 5 \mod 12 \end{aligned}$$

- $a = 6, n = 13$

$$\begin{aligned} a^{-1} &= a^{p-2} \mod p \quad \text{if } p \text{ is prime} \\ 6^{-1} &= 6^{13-2} \mod 13 \\ &= 6^{11} \mod 13 = 11 \end{aligned}$$

Exercise 6

Solve problem 7.1 on page 200. Show the details of the computations. Let the two primes $p = 41$ and $q = 17$ be given as set-up parameters for RSA.

1. Which of the parameters $e_1 = 32, e_2 = 49$ is a valid RSA exponent? Justify your choice.

$$\begin{aligned} n = pq &= 41 \times 17 = 697 \\ \phi(n) &= (p-1)(q-1) = 640 \\ gcd(\phi(n), e_1) &= gcd(640, 32) = 32 \\ gcd(\phi(n), e_2) &= gcd(640, 49) = 1 \end{aligned}$$

   $e_2 = 49$ is a valid choice because it is coprime to $\phi(n)$.

2. Compute the corresponding private key $K_{pr} = (p, q, d)$. Use the extended Euclidean algorithm for the inversion and point out every calculation step.

$$\begin{aligned} \phi(n) &= 640 \quad e = 49 \\ de &\equiv 1 \mod \phi(n) \\ 640 &= 13 \times 49 + 3 \\ 49 &= 16 \times 3 + 1 \\ gcd(640, 49) &= 1 \\ 1 &= 49 - 16 \times 3 \\ &= 49 - 16 \times (640 - 13 \times 49) \\ &= 209 \times 49 - 16 \times 640 \\ &= 209 \times 49 \mod 640 \\ d &= e^{-1} = 209 \end{aligned}$$

Exercise 7

Solve problem 7.2 on page 200. Show the details of the computations. Computing modular exponentiation efficiently is inevitable for the practicability of RSA. Compute the following exponentiations $x^e \mod m$ applying the square and multiply algorithm:

1. $x = 2, e = 79, m = 101$

$$79 = 1001111_2$$

Step	Accumulated Result	Binary Exponent
1	$r = 1^2 \times 2 \equiv 2 \mod 101$	1
2	$r = 2^2 \equiv 4 \mod 101$	10
3	$r = 4^2 \equiv 16 \mod 101$	100
4	$r = 16^2 \times 2 \equiv 7 \mod 101$	1001
5	$r = 7^2 \times 2 \equiv 98 \mod 101$	10011
6	$r = 98^2 \times 2 \equiv 18 \mod 101$	100111
7	$r = 18^2 \times 2 \equiv 42 \mod 101$	1001111

$$2^{79} \mod 101 = 42$$

2. $x = 3, e = 197, m = 101$

$$197 = 11000101_2$$

Step	Accumulated Result	Binary Exponent
1	$r = 1^2 \times 2 \equiv 2 \mod 101$	1
2	$r = 2^2 \times 2 \equiv 8 \mod 101$	11
3	$r = 8^2 \equiv 64 \mod 101$	110
4	$r = 64^2 \equiv 56 \mod 101$	1100
5	$r = 56^2 \equiv 5 \mod 101$	11000
6	$r = 5^2 \times 2 \equiv 50 \mod 101$	110001
7	$r = 50^2 \equiv 76 \mod 101$	1100010
8	$r = 76^2 \times 2 \equiv 38 \mod 101$	11000101

$$2^{197} \mod 101 = 38$$

Exercise 8

Solve problem 7.3 on page 200. Show the details of the computations. Encrypt and decrypt by means of the RSA algorithm with the following system parameters:

- $p = 3, q = 11, d = 7, x = 5$

$$\begin{aligned} n &= pq = 33 \\ \phi(n) &= \phi(33) = (11-1)(3-1) = 20 \\ de &\equiv 1 \mod \phi(n) \\ e &= d^{-1} \mod \phi(n) = 3 \mod 20 \\ y &= x^e \mod n = 5^3 \mod 33 = 26 \end{aligned}$$

- $p = 5, q = 11, e = 3, x = 9$

$$
\begin{aligned}
n &= pq = 55 \\
\phi(n) &= \phi(55) = (11-1)(5-1) = 40 \\
de &\equiv 1 \mod \phi(n) \\
d &= \mathrm{e}^{-1} \mod \phi(n) = 27 \mod 40 \\
y &= x^d \mod n = 9^{27} \mod 55 = 4
\end{aligned}
$$

If you have any questions, comments, or concerns, please contact me at alvin@omgimanerd.tech