Q1, Find the prime factorization of 27999510 using the **Sieve of Eratosthenes**.

Start with the numbers 2 to 27999510.

Mark 2 as prime and cross out all its multiples (except itself).

Continue with 3, 5, 7,...

Repeat this process until you reach the square root of 27999510, which is about 5291.

All the remaining unsigned numbers in the list are primes.

Find the prime factors of 27999510 by dividing it by each prime in increasing order until the quotient is 1.

We have:

* 27999510 / 2 = 13999755
* 13999755 / 3 = 4666585
* 4666585 / 5 = 933317
* 933317 / 7 = 133331
* 133331 can’t devide by 9
* 133331 / 11 = 12121
* 12121 can’t devide by 13
* 12121 / 17 = 713
* 713 can’t devide for 19
* 713 / 23 = 31
* 31 is prime number, so 31 / 31 = 1

==> 27999510 = 2\*3\*5\*7\*11\*17\*23\*31

Q2, MESSAGE = “**NZQLIG**”  
Key = 8

Base on English Alphabet, we decrypt the message:

Left shift of ‘N’ with k = 8 is ‘F’

Left shift of ‘Z’ with k = 8 is ‘R’

Left shift of ‘Q’ with k = 8 is ‘I’

Left shift of ‘L’ with k = 8 is ‘E’

Left shift of ‘I’ with k = 8 is ‘A’

Left shift of ‘G’ with k = 8 is ‘Y’

==> After decrypt the message with k = 8, we have word “FRIEAY”

Q3, MESSAGE = “**ZBAQNL**”  
Because the English Alphabet have 26 characters and in Caesar Cipher, we can have 26 cases for left shift or right sift. In the worst case we don’t have key, we must solve 26 cases for all to perform to reach to the plaintext.

Q4, MESSAGE = “**ONKEDGEXGHTITSTXOIAM**”

Permutation Cipher with key [3 5 1 2 4]

Create the table for message and key, we have:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| O | N | K | E | D | G | E | X | G | H | T | I | T | S | T | X | O | I | A | M |
| 3 | 5 | 1 | 2 | 4 | 3 | 5 | 1 | 2 | 4 | 3 | 5 | 1 | 2 | 4 | 3 | 5 | 1 | 2 | 4 |

Encrypt the message, we have: “KXTIEGSAOGTXDHTMNEIO”

Q5, Find the prime factorization of 135, we have: 135 = 33\*5

==> The Euler totient function of 135 is: totient(135) = 135\*(1-1/3)\*(1-1/5) = 72

Q6, We have:

p = 5, q = 17, e = 7

==> phi(n) = (p-1)\*(q-1) = 4\*16 = 64

So the value of phi(n) for the RSA cipher is 64.

Q7, We have:

p = 5, q = 17, e = 7

d = 55, M = 3

We have:

n = p\*q = 85

M = 3

C = Me mod n = 37 mod 85 = 62

==> Ciphertext C = 62

Q8, p = 5, q = 17, e = 7

c' = c\*r^e mod n = 23\*128 mod 85 = 23\*27 mod 85 = 54

==> r = 2, n = 85, phi(n) = 64

We have c = Me mod n or M = cd mod n

The private key d is calculated by finding an integer that satisfies the equation

* e\*d mod phi(n) = 1

<=> 7d mod 64 = 1

One way to do this is to use the **Extended Euclidean algorithm**, which finds integers x and y such that **ax + by = gcd(a,b).**

In this case, we have 7x + 64y = gcd(7,64) = 1

Solve the equation, we find x = -9 and y = 1. Since we want a positive value for d, we can add 64 to x and get d = -9 + 64 = 55.

==> M = cd mod n = 2355 mod 85

We have:

* 235 mod 85 = 58
* 2310 mod 85 = (235)2 mod 85 = 582 mod 85 = 49
* 2350 mod 85 = (2310)5 mod 85 = 495 mod 85 = 19
* 2355 mod 85 = (2350 \* 235) mod 85 = (58\*19) mod 85 = 82

==> M = 2355 mod 85 = 82

Q9, We have:

p = 17, root a = 3, Y\_A=11

We have:

Y\_A = aX\_A mod p

<=> 11 = 3X\_A mod 17

With p = 17, X\_A get value in range (0;16)

Solve with each value, we have:

* 30 mod 17 = 1
* 31 mod 17 = 3
* 32 mod 17 = 9
* 33 mod 17 = 10
* 34 mod 17 = 13
* 35 mod 17 = 5
* 36 mod 17 = 15
* 37 mod 17 = 11

==> X\_A = 7

Q10, We have 7 computers, each computer hosts 3 virtual machines, and each VM hosts 6 applications.

Because all virtual machines need shared pair-wise keys, each virtual machine needs to have a master key that is shared with every other virtual machine.

Because there are 7 computers, each hosting 3 virtual machines, so a total is 7\*3 = 21 virtual machines. We have the formula to calculator: N\*(N-1)/2

Therefore, there are (21\*20)/2 = 210 primary keys required for all virtual machines.