1, Find the prime factorization of 9699690 using the sieve of Eratosthenes.

Start with the numbers 2 to 9699690.

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 9699690, which is about 3114.

All the remaining unsigned numbers in the list are primes.

Find the prime factors of 9699690 by dividing it by each prime in increasing order until the quotient is 1.

We have:

* 9699690 / 2 = 4849845
* 4849845 / 3 = 1616615
* 1616615 / 5 = 323323
* 323323 / 7 = 46189
* 46189 / 11 = 4199
* 4199 / 13 = 323
* 323/17 = 19
* 19 / 19 = 1

==> 9699690 = 2x3x5x7x11x13x17x19

1, 69^(totient(377)) = 69^336 = 1 (mod 377)

Then we can write:

69^673 = (69^336) \* (69^(336 + 1)) \* (69^(336 - 1))

= (1) \* (69) \* (69^-1) (mod 377)

= 69 \* (69^-1) (mod 377)

= 1 (mod 377)

Therefore, the answer is:

69^673 mod 377 = 1

2, MESSAGE = “QAMMGWC”  
Key = 8

Base on English Alphabet, we decrypt the message:

Left shift of ‘Q’ with k = 8 is ‘I’

Left shift of ‘A’ with k = 8 is ‘S’

Left shift of ‘M’ with k = 8 is ‘E’

Left shift of ‘G with k = 8 is ‘Y’

Left shift of ‘W’ with k = 8 is ‘O’

Left shift of ‘C’ with k = 8 is ‘U’

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

3, MESSAGE = “QAMMGWC”  
Because in Caesar Cipher, we can have 26 cases for left shift or right sift and in the worst case we don’t have key, we must solve 26 cases for all to decrypt the message.

4, MESSAGE = “SEEYOUTOMORROW”

Permutation Cipher with key [5 3 1 2 4]

Create the table for message and key, we have:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| S | E | E | Y | O | U | T | O | M | O | R | R | O | W |
| 5 | 3 | 1 | 2 | 4 | 5 | 3 | 1 | 2 | 4 | 5 | 3 | 1 | 2 |

Encrypt the message, we have: “EOOYMWETROOSUR”

5, Find the prime factorization of 50, we have: 50 = 2\*52

==> The Euler totient function of 50 is: totient(50) = 50\*(1-1/2)\*(1-1/5) = 20

6, p = 13, q = 17, e = 5

==> phi(n) = (p-1)\*(q-1) = 192

So the value of phi(n) for the RSA cipher is 192.

7, p = 13, q = 17, e = 5

d = 269, M = 6

We have:

n = p\*q = 221

M = 6

C = M^e mod n = 65 mod 221 = 41

==> Ciphertext C = 41

7, p = 5, q = 13, e = 5

d = 29, M = 17

We have:

n = p\*q = 65

M = 17

C = M^e mod n = 175 mod 65 = 62

==> Ciphertext C = 62

8, p = 5, q = 13, e = 5

c' = c\*r^e mod n = 19\*243 mod 65 = 19\*35 mod 65 = 2

==> r = 3, n = 65, phi(n) = 48

We have c = M^e mod n or M = c^d mod n

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

e\*d mod phi(n) = 1

<=> 5d mod 48 = 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 5x + 48y = gcd(5,48) = 1

Solve the equation, we find x = -19 and y = 2. Since we want a positive value for d, we can add 48 to x and get d = -19 + 48 = 29.

==> M = c^d mod n = 19^29 mod 65

We have:

192 = 36 (mod 65)

195 = 54 (mod 65)

197 = 59 (mod 65)

199 = 44 (mod 65)

1910 = 56 (mod 65)

1920 = 16 (mod 65)

==> 1929 = 54 (mod 65)

==> M = 54

8, p = 7, q = 13, e = 7

c' = c\*r^e mod n = 18\*128 mod 91 = 18\*27 mod 91 = 29

==> r = 2, n = 91, phi(n) = 72

We have c = m^e mod n or m = c^d mod n

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

e\*d mod phi(n) = 1

<=> 7d mod 72 = 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 + 72y = gcd(7,72) = 1

Solve the equation, we find x = -41 and y = 4. Since we want a positive value for d, we can add 72 to x and get d = -41 + 72 = 31.

==> m = c^d mod n = 18^31 mod 91

We have:

181 = 18 (mod 91)

185 = 44 (mod 91)

1810 = 25 (mod 91)

1830 = 64 (mod 91)

1831 = 60 (mod 91)

==> 1831 =60 (mod 91)

==> m = 60

9, p = 13, root a = 2, Y\_A=3

We have:

Y\_A = aX\_A mod p

<=> 3 = 2X\_A mod 13

With p = 13, X\_A get value in range (0;12)

Solve with each value, we have 24 = 3 (mod 13)

==> X\_A = 4

9, p = 13, root a = 2, Y\_A=9

We have:

Y\_A = aX\_A mod p

<=> 9 = 2X\_A mod 13

With p = 13, X\_A get value in range (0;12)

Solve with each value, we have 28 = 9 (mod 13)

==> X\_A = 8

10, We have 8 computers, each computer hosts 4 virtual machines, and each VM hosts 10 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 8 computers, each hosting 4 virtual machines, so a total is 8\*4 = 32 virtual machines.

Therefore, there are (32\*31)/2 = 496 primary keys required for all virtual machines.