1.

Plain text: INFORMATION SECURITY

Caesar cipher table:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

Ciphertext : F K C L O J X Q F L K P B Z R O F Q V

2.

First, converting those numbers to binary as follows

13 -> 1101

8 -> 1000

4 -> 0100

Therefore,

13 will become 0000 -> 0

8 will become 1101 -> 13

4 will become 1010 -> 10

3.

Because 7 and 23 are relative primes, 7 has its multiplicative inverse.

23 =7*3 + 2 *and* 7 = 3*2+1
So 1 = 7 – 3*2 = 7 – 3*(23 – 7*3) = 7(10) – 23(3) From 23(3) + 1 = 7(10) , the multiplicative inverse of 7 is 10.

4.

Gcd(512,240) = gcd(240, 512 mod 240) =>gcd(240, 32)

=gcd (32, 240 mod 32) =>gcd(32,16)

=gcd(16,32 mod 16) =>gcd(16,0)

gcd(512,240) = 16

Therefore, the gcd of 512 and 240 is 16.

5.

M=9, k=4, (p,g,y)=(59,2,25)

a = g^k mod p = 2^4 mod 59 = 16

b = My^k mod p = (9)(25^4) mod 59 = 51

encryption of M = (16,51)

6.

H(x) = (5x + 11) mod 19

H(4) = (20+11) mod 19 = 12

19y+12-11 = 5x => 19y+1 = 5x, 19y+1 has to be multiples of 5

Search for 19y value where 19y+1 mod 5 = 0

19*6=114, 114+1/5 = 23

19*11=209 209+1/5 = 42

19*16=304 304+1/5= 61

19*21=399 399+1/5 = 80

H(23),H(42),H(61),H(80) all has same hashed value, the hash function is not weakly collision resistant.

7.

20^10211 mod 10401

Euler’s method

10401 = 3 * 3467, (both numbers are prime numbers)

10401(1- 1/3) (1-1/3467) = 24040178 mod 10401 = 6932

10211 mod 6932 = 3279

20^3279 mod 10401 = 3299

Confirmation:

20^10211 =

20^(2^13) + 20^(2^10)+ 20^(2^9) +20^(2^8) +20^(2^7)
+20^(2^6)+20^(2^5)+20^(2^1)+20^(2^0)

=1582*7255*9187*3847*157*2149*7249*400*20 mod 10401 = 3299