密碼學概論 HW4 0410180 何秉諺

1.

當a = 3時 產生數列

3 9 27 19 26 16 17 20 29 25 13 8 24 10 30 28 22 4 12 5 15 14 11 2 6 18 23 7 21 1

總共有30個不重複數、period = 30

當a = 32時 產生數列 產生的period = 15

9 19 16 20 25 8 10 28 4 5 14 2 18 7 1 9 19 16 20 25 8 10 28 4 5 14 2 18 7 1

因為k = 2 和 m – 1 並非互質，所以無法產生最大period 30

當a = 33時 因為 3和30非互質，產生的period = 10

27 16 29 8 30 4 15 2 23 1 27 16 29 8 30 4 15 2 23 1 27 16 29 8 30 4 15 2 23 1

當a = 34時 因為 4和30非互質，產生的period = 15

19 20 8 28 5 2 7 9 16 25 10 4 14 18 1 19 20 8 28 5 2 7 9 16 25 10 4 14 18 1

2.

A) compute RC4( v || k ) , then Xor c

B) try the key k to v1 and test RC4(v1,k) XOR c1 , if the c1 decrypted , use it to

RC4(v2, k) to test whether it decrypted , too . if decrypted , then the same key stream has been used to encrypt two messages .

C)

D)

3.

A)

pair 00: (0.5-p)2 pair 10: (0.5+p)(0.5-p)

pair 01: (0.5-p)(0.5+p) pair 11: (0.5+p)2

B)

P(01) = ------------------- = 0.5

P(10) = ------------------- = 0.5

C)

The probability of non-discard bit :

所以total expected # = -------------

4.

E = 13 , n = 77 , c = 20

n(77) = 60 , 13d = 1 mod 60 for d=37

find C37 mod 77 = 2037 mod 77

因為 2010 mod 77 = 1

207 mod 77 = 48

所以 2037 mod 77 = 48

5.

Calculate 6472 mod 3415

472 = 111011000(2) = 8 + 16 + 64 + 128 + 256

62 % 3415 = 12 64 % 3415 = 1296

68 % 3415 = 2851 616 % 3415 = 501

632 % 3415 = 1706 664 % 3415 = 856

6128 % 3415=1926 6256 % 3415 = 786

所以6472 % 3415 = (786\*1926\*856\*501\*2851)%3415 = 3346

6.

A) 515 mod 157

= (55 mod 157)3 mod 157

= 1423 mod 157 = 79

B) 527 mod 157

= (59 mod 157)3 mod 157

= 453 mod 157 = 65

6.C)

7927 mod 157 = (793)9 mod 157

= 599 mod 157 = 233 mod 157

= 78

6515 mod 157 = (653)5 mod 157

= (32)5 mod 157

= 78

Secret key : 78

7.

A)

K = 103 mod 157 = 58

C1 = 53 mod 157 = 125

C2 = 58\*9 mod 157 = 51

Ciphertext = ( 125, 51)

B)

C1 = 25 = 55 mod 157

K = 105 mod 157 = 148

C2 = 148 \* 9 mod 157 = 76

8. find (x,y) in y2 mod 7 = x3 + 2x + 1 mod 7 for Z7

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| X = | x3 + 2x + 1 mod 7 | Y = | y2 mod 7 | *Point in E7* |
| 0 | 1 | 0 | 0 | *(0,1)* |
| 1 | 4 | 1 | 1 | *(0,6)* |
| 2 | 6 | 2 | 4 | *(1,2)* |
| 3 | 6 | 3 | 2 | *(1,5)* |
| 4 | 3 | 4 | 2 |  |
| 5 | 3 | 5 | 4 |
| 6 | 5 | 6 | 1 |