Brendan Forbes

Cryptography

Homework 2 Part b

* 1. YA= 7^5 mod 71 = 51
  2. YB = 7^12 mod 71 = 4
  3. The shared secret key is YB^XA (mod 71) = YA^XB (mod 71) = 58
  4. In this case, both public keys would be 25, the computed shared keys would be 1 and 57 which are not the same
  5. Generate 2^32 variations of a valid message with essentially the same meaning and 2^32 variations of a desired fraudulent message. Messages are compared to find pair with same hash. The user will sign one of the valid messages and forgery can then be substituted
  6. 2^33\*M bits
  7. 2^32/2^20 = 4096 seconds or roughly 68 minutes
  8. Memory=2^65\*M bits & 2^64/2^20=1.76\*10^13 s or roughly 550,000 years

1. Encryption:

S= {5, 9, 21, 45, 103, 215, 450, 946}; a = 1019; p = 1999

Ti = a\* Si (mod p)

T = {1097, 1175, 1409, 1877, 1009, 1194, 779, 456}

P = {0, 1, 0, 1, 0, 1, 1, 1}

Y = 1175 + 1877 + 1194 + 779 + 456 = **5481**

Decryption:

Y = 5481

a^(-1) = 1999 – 410 = 1589

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| T | Ot | R | Or | Q |
| 1 | 0 | 1019 | 1999 | 1 |
| -1 | 1 | 980 | 1019 | 1 |
| 2 | -1 | 39 | 980 | 25 |
| -51 | 2 | 5 | 39 | 7 |
| 359 | -51 | 4 | 5 | 1 |
| -410 | 359 | 1 | 4 | 4 |
|  | -410 | 0 | 1 |  |

Z = a^(-1) Y (mod P) = 1589\*5481 (mod 1999) = 1665

Subset Sum I(S, Z) = {\_, 9, \_, 45, \_, 215, 450, 946}

Therefor P = {0, 1, 0, 1, 0, 1, 1, 1}