Danil Badarev, s3210928 / Jens Taken, s3136027

**5.6**

a) We started by counting the occurrence of the letters in the sentence. Using frequency analysis we came to the conclusion that B must represent E. Meaning the key must equal 3. Meaning EBOBFPXKBKDIFPEPBKQBKZBQEXQZLKQXFKPJLOBLCQEBIBQQBOBQEXKLCXKVLQEBOIBQQBO would translate into: HEREISANENGLISHSENTENCETHATCONTAINSMOREOFTHELETTERETHANOFANYOTHERLETTER.

b) AJTSHJIVFYWXJVRSHOLVKQZWFSKZXUWRTSHZEQIFMGXIFKJPPYQTVWFWHOLRXMMWGHIVVYSWNMTFQZRG

AJTSH JIVFY WXJVR SHOLV KQZWF SKZXU WRTSH ZEQIF MGXIF KJPPY QTVWF WHOLR XMMWG HIVVY SWNMT FQZRG

We noticed that HIVVY and PEARL give the key SEVEN in the table. Using a hint we knew that we had to look for a word with length 5, so we started comparing the word PEARL with every 5 letter combination from our cipher. Meaning this sentence would translate into: IFYOUREABLETOREADTHISMESSAGETHENYOUHAVESUCCESSFULLYPASSEDTHEFIRSTPEARLASSIGNMENT

5.7)

14-7-27-27-9-25 letters -> decimals

01110- 00111-11011-11011-01001-11001 decimals -> binary

011-100-011-111-011-110-110-100-111-001 “shift” r=3

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 3-bits | IV | IV decimal | EK(IV) = 3 \* IV + 2 \* 13 mod 32 | XOR 3 bits EK(IV) |
| 011 | 10110 | 22 | 11100 | 100 |
| 100 | 11100 | 28 | 01110 | 111 |
| 011 | 01110 | 14 | 00100 | 010 |
| 111 | 00100 | 4 | 00110 | 110 |
| 011 | 00110 | 6 | 01100 | 000 |
| 110 | 01100 | 12 | 11110 | 001 |
| 110 | 11110 | 30 | 10100 | 011 |
| 100 | 10100 | 20 | 10110 | 001 |
| 111 | 10110 | 22 | 11100 | 000 |
| 001 | 11100 | 28 | 01110 | 010 |

100-111-010-110-000-001-011-001-000-010

10011-10101-10000-00101-10010-00010

19 21 16 5 18 2 -> SUPERB

5.8 )

Phi (n) = (p-1)(q-1)

N = p\*q

q = N/p

Phi (n) = (p-1)(q – 1)

Phi (n) = pq – p - q + 1

Phi (n) = N - p – N/p + 1

p + N/p = N+1 – phi(n) |\*p

p^2 + N = p(N+1 – Phi(n))

p^2 – p(N+1 – phi(n)) + N = 0

a = 1, b = N +1 - phi(N), c = N

X = -b +/- sqr (d) / 2a where d = b^2 – 4a

p,q = (N+1-Phi(n) +- sqrt((N+1-Phi(n))^2 - 4N))/2

5.9)

a) N = pq = 47 \* 61 = 2867

Phi(n) = (p-1)(q-1) = (46 \* 60) = 2760

e=7. Because gcd (7, 2760) = 1

pk = (N,e) = (2867, 7)

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

Knowing that: Fi(n)*x + e*y = gcd(Fi(n), e) =>2760*x + 7*y = 1 we should find y using

Extended Euclidean Algorithm:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **q** | **r** | **x** | **y** | **a** | **b** | **x2** | **x1** | **y2** | **y1** |
| 0 | 0 | 0 | 0 | 2760 | 7 | 1 | 0 | 0 | 1 |
| 394 | 2 | 1 | -394 | 7 | 2 | 0 | 1 | 1 | -394 |
| 3 | 1 | -3 | 1183 | 1 | 1 | 1 | -3 | -394 | 1183 |
| 2 | 0 | -5 | -2760 | 1 | 0 | -3 | -5 | 1183 | -2760 |

So the secret key D = 1183

c)

The ciphertext = E (m, e) = m^e mod N = 5^7 mod 2867 = 716

d)

s = 9, e = 7,d = 395, N = 2867, and m = 813

m’ = E(s, e) = s^e mod N = 9^7 mod 2867 = 4 782 969 mod 2867 = 813 = m => the signature s=9 is a valid RSA signature