Two other Crypto Challenges

I wrote two other crypto challenges, redoing some of the cryptanalysis problems in [1]. Hope you enjoy it.

Question One

Let us take a quick recap of the RSA cryptosystem before we proceed to the
challenge.

```
RSA key generation
-------------------
(1)Generate two large random primes, p and q.
Compute n = pq and the Euler Totient Function phi(n) = (p-1)(q-1).
(2)Choose an integer e, 1 < e < phi(n), such that gcd(e, phi(n)) = 1.
(3)Compute d=inverse(e) modulo phi(n).
The public key is (e, n) and the private key is (d,n).

Let P be the plaintext.

Encryption step
---------------
(4)Ciphertext C = P^e modulo n.

Decryption step
---------------
(5)Plaintext P = C^d modulo n.
```

Now,lets get down to the challenge.We know

```
n=p*q=
326876483856375377836408113541818740612158979784333325058933
357238058959978186381151707161630923720156506333606757577356
348897777862803515902246025225890311618086597583349
and
phi(n)=326876483856375377836408113541818740612158979784333325058933
357238058959978186380381796500954286944382260885931091253678968820310
5991194157416927152440676498542899865642 36
```

It is known that either p or q has been used in other cryptosystems for key
generation. Our task is to find the values of p and q and save the day!

Solution to Question One

Congratulations to Furcalor for trying it out and solving it correctly.

Furcalor wrote:

Well anyway basically it goes like this

As you said:

n=
32687648385637537783640811354181874061215897978433332505893357238058959978186381151707161630923720156506333606757577356348897777862803515902246025225890311618086597583349

phi(n)=32687648385637537783640811354181874061215897978433332505893357238058959978186380381796500954286944382260885931091253678968820310599119415741692715244067649854289986564236

So:

p=
[n+1-phi(n)+sqrt((n+1-phi(n))^2-4n)]/2
=
769910660634180358352109076984911579855410179367854966867943645928713697465636771478367287

and q=
[n+1-phi(n)-sqrt((n+1-phi(n))^2-4n)]/2

=
42456417422136370690754743821969898099408717232216907381268125196127025132651827

And to verify:

N=769910660634180358352109076984911579855410179367854966867943645928713697465636771478367287
*
42456417422136370690754743821969898099408717232216907381268125196127025132651827
=
32687648385637537783640811354181874061215897978433332505893357238058959978186381151707161630923720156506333606757577356348897777862803515902246025225890311618086597583349

End of Furcalor's comment.

Let us see if Furcalor's approach can be understood a little more systematically.

We have n=p*q.

phi(n)=(p-1)*(q-1)
phi(n)=(p*q)-p-q+1
phi(n)=n-(p+q)+1.
Call (p+q)=2b, this is always true since p+q is even and hence 2 is a factor.
Therefore, 2*b=n+1-phi(n) which can easily be found since n and phi(n) are given.

All that remains is to find the roots of the quadratic equation
x^2 -2*b*x +n = 0, with sum of roots as 2*b and product of roots as n.

The solutions are
p,q=[2*b(+ or -)squareroot((4*b^2) - (4*n))]/2

=b(+ or -)squareroot(b^2 - n)

P.S: We thank R.S for providing the large primes used in this challenge.

Question Two

We know that our adversary is using a 2*2 enciphering matrix with a 29-letter alphabet scheme.

The conventional encodings are: [A-Z]=[0-25], blank_space=26, ?=27, !=28.
We intercept the encrypted message

IK!UZ FM!FP (Note there are two black_spaces in between).

Since the message is signed by BOND, we know that

```
|         |      |          |
| B    N  |      | M     F  |
|         | <==> |          |
| O    D  |      | !     P  |
|         |      |          |
```

i.e. M==>B, !==>O, F==>N, P==>D.

We also know that all encryptions are of the form:
Enc_key * Plain_Text = Cipher_Text.

and all decryptions are of the form:
Dec_key * Cipher_Text = Plain_Text

Find the Plain_Text and save the day.

Solution to Question Two

We know

```
  Dec_key *| M      F | = | B    O |
           | !      P |   | N    D |
```

or

```
  Dec_key =  | 1    13 | * Inverse| 12    5  |
             | 14    3 |          | 28   15  |,
```

We know the Inverse of the Matrix is the Adjont of the matrix divided
by its determinant. Therefore,

```
Inverse| 12    5 | = (1/11)*  | 15     24  | = | 4      18 |
       | 28   15 |            |  1     12  |   | 8       9 |
```

Therefore,

```
  Dec_key =  | 1    13 | * | 4    18  | = | 21     19 |
             | 14    3 |   | 8     9  |   | 22     18 |
```

We now retreive the Plain_Text as follows:

We know

```
  | I   !  | =  |  8    28 |
  | K   U  |    | 10    20 |
```

Therefore,

```
  Dec_key*  |  8    28  | =  Plain_Text1
            | 10    20  |
```

```
|  21    19 |*|  8    28 | = | 10    11  | = | K    L |
|  22    18 | | 10    20 |   |  8    19  |   | I    T |
```

We also know,

```
| Z      blank | = | 25    26 |
| blank      F |   | 26     5 |
```

Therefore,

```
Dec_key*  | 25    26 | =  Plain_Text2
          | 26     5 |

|  21    19 |*|  25  26| = | 4     3 | =  | E     D |
|  22    18 | |  26   5|   | 3    24 |    | D     Y |
```

Concatenating Plain_Text1 and Plain_Text2, we get
KILTEDDY ,which is to to be read as KIL TEDDY as signed by BOND.

Bibliography

[1.] A Course in Number theory and Cryptography, Graduate Text in Mathematics, Neal Koblitz.

-Sarad A.V