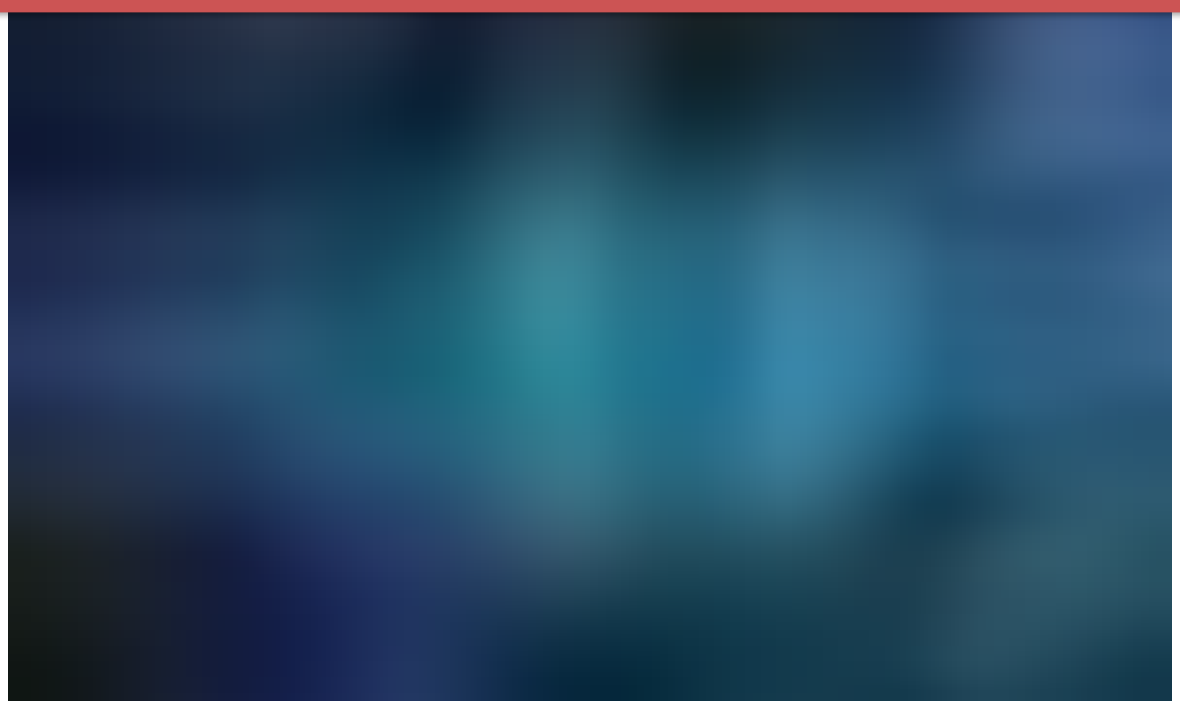


Cracking RSA — A Challenge Generator

Prof Bill Buchanan OBE Follow

Aug 27, 2018 · 2 min read ★

Do you have what it takes to be a cipher cracker? Well here is a challenge for you [here]:

```
RSA Encryption parameters. Public key: [e,N].
e: 65537
N: 498702132445864856509611776937010471
Cipher: 967083045009025409276826017096679 39
We are using 60 bit primes


Can you find the value of the message?
```

With this we are using the RSA encryption method, and we have the encryption key (e,N). We must find the two prime numbers which create the value of N (p and q), and must use a factorization program to find them. Once we find the factors it is easy to then determine the decryption key (d,N).

Example

Here is an example:

```
Encryption parameters
e:      65537
N:      1034776851837418228051242693253376923
Cipher: 582984697800119976959378162843817868
We are using  60 bit primes
```

Now we have to crack N by finding the primes that make up the value.

If we use this [link], we get:

```
Factors
-------
1,034,776,851,837,418,228,051,242,693,253,376,923 =
1,086,027,579,223,696,553 x 952,809,000,096,560,291
```

p=1,086,027,579,223,696,553 q=952,809,000,096,560,291

Now we work out PHI, which is equal to $(p-1)\times(q-1)$:

```
>>>p=1086027579223696553
>>>q=952809000096560291
>>> print (p-1)*(q-1)
1034776851837418226012406113933120080
```

Now we find $e^{-1} \pmod{PHI}$ (and where $(d\times e) \pmod{PHI}=1$), such as using [here]:

```
Inverse of  65537  mod
1034776851837418226012406113933120080
Result: 568411228254986589811047501435713
```

This is the decryption key. Finally we decrypt with $Message = Cipher^{d} \pmod{N}$:

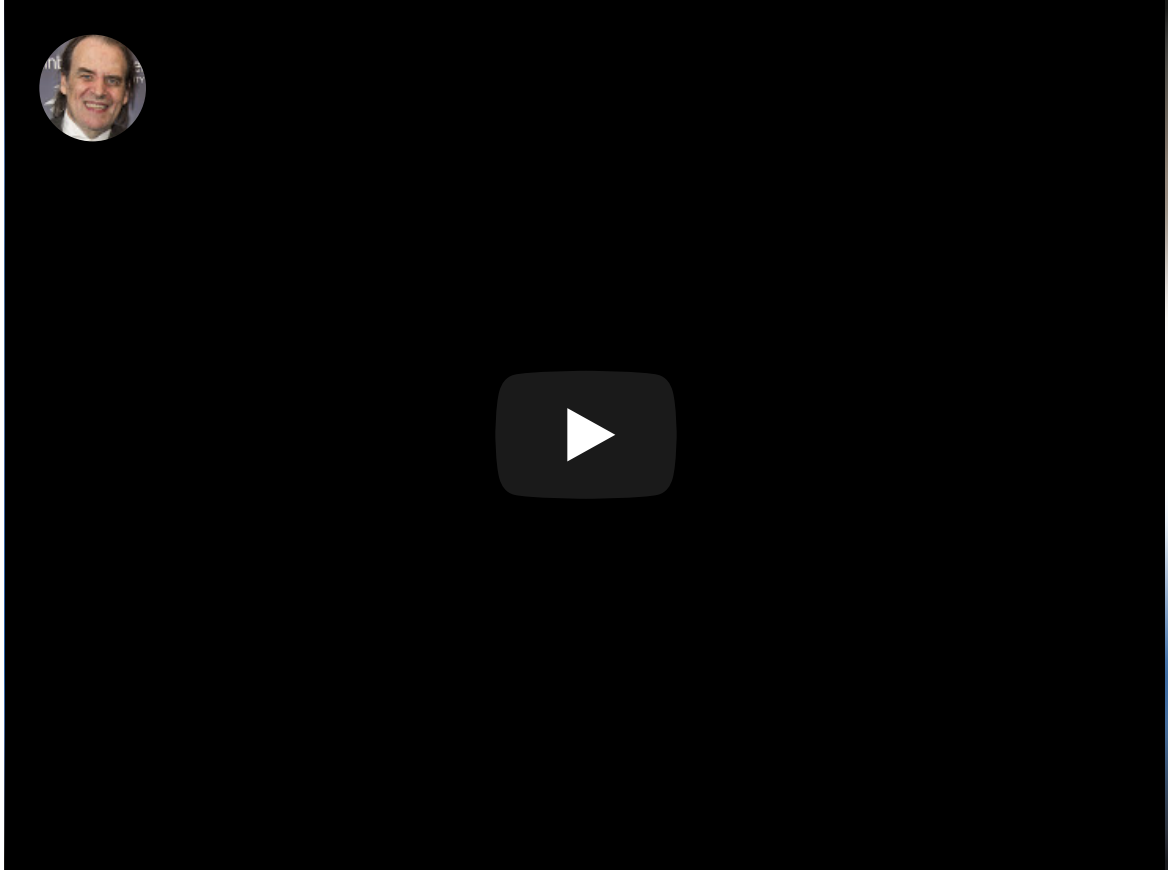
```
>>> d=568411228254986589811047501435713
>>> cipher=582984697800119976959378162843817868
>>> N=1034776851837418228051242693253376923
>>> print pow(cipher,d,N)
345
```

The message is 345

Finally, let's check the answer. So we can re-cipher with the encryption key and we use $Cipher = M^{e} \pmod{N}$:

```
>>> m=345
>>> e=65537
>>> N=1034776851837418228051242693253376923
>>> print pow(m,e,N)
582984697800119976959378162843817868
```

This is the same as the cipher, so the encryption and decryption keys have worked. Thus the encryption key is [65537, 1034776851837418228051242693253376923] and the decryption key is [568411228254986589811047501435713, 1034776851837418228051242693253376923]



Conclusions

This is fairly simple to compute as the prime numbers are fairly small. In real-life these will be 1,024 bit prime numbers, and N will have 2,048 bit numbers, which will be extremely difficult to factorize.

If you want here's some challenges:

1. Challenge with 60-bit primes:

```
RSA Encryption parameters. Public key: [e,N].
e: 65537
N: 911844725340031776516886332975892441
Cipher: 801127314512167104045686292190207406
We are using 60 bit primes
```

```
Can you find the value of the message?
```

2. Challenge with 80-bit primes:

```
RSA Encryption parameters. Public key: [e,N].
e: 65537
N: 115717097310257568301673641106204976164329204539 7
Cipher: 398616441584847118291875619819339172891325623639
We are using 80 bit primes
```

```
Can you find the value of the message?
```

3. Challenge with 128-bit primes:

```
RSA Encryption parameters. Public key: [e,N].
e: 65537
N:
491419399311372611168437753627833986739312580319238952832863
20973486872970729
Cipher:
141991237870468300480669722900521367694153568249816958363606
04590953658335413
We are using 128 bit primes

Can you find the value of the message?
```

———————————————-

———————————————-

Answers

———————————————-

1. Answer is: 1497

2. Answer is: 427

2. Answer is: 145