Chosen Cipher Attack

[Back] In this attack Eve gets Bob to cipher a chosen ciphertext. First Eve captures some cipher text, and then sends this back (with a random value raised to the power of Bob's encryption key (e)) and if Eve can determine the decrypted value, she can crack the message:

Parameters

Message: 10

Random (r): 3

Keys

e: 79 d: 1019 N: 3337

Determine

- Message=32, r=5, e= 79 d= 1019 N= 3337 Try!
- Message=50, r=6, e= 79 d= 1019 N= 3337 Try!
- Message=100, r=8, e= 79 d= 1019 N= 3337 Try!
- Message=200, r=10, e= 79 d= 1019 N= 3337 Try!
- Message=50, r=2, e=7, d=503, N=943 Try!
- Message=200, r=3, e=7, d=503, N=943 Try!
- Message=200, r=3, e=7, d=503, N=943 Try!
- Message=100, r=5, e=7, d=503, N=943 Try!
- Message=200, r=3, e=17, d=2753, N=3233 Try!
- Message=100, r=5, e=17, d=2753, N=3233 Try!
- Message=19, r=4, e=17, d=2753, N=3233 Try!
- Message=50, r=2, e=7, d=103, N=143 Try!

Some worked examples of RSA keys are [here]

```
==Initial values ====
e= 79 d= 1019 N= 3337
message= 10 r= 3

=============
Initial cipher: 3269
Eve gets Bob to decipher:  2604 (Cipher *
r^e mod N)
Bob says that the result is: 30

=============
Eve determines the message as: 10
Eve has cracked message, as result is same
as message
```

Outline

First Eve listens for a cipher that she want to crack:

$$C = M^e \mod N$$

Next she takes this cipher and gets Bob to decrypt it (and also multiplying by a random value to the power of Bob's e value):

$$C' = C \times r^e \mod N$$

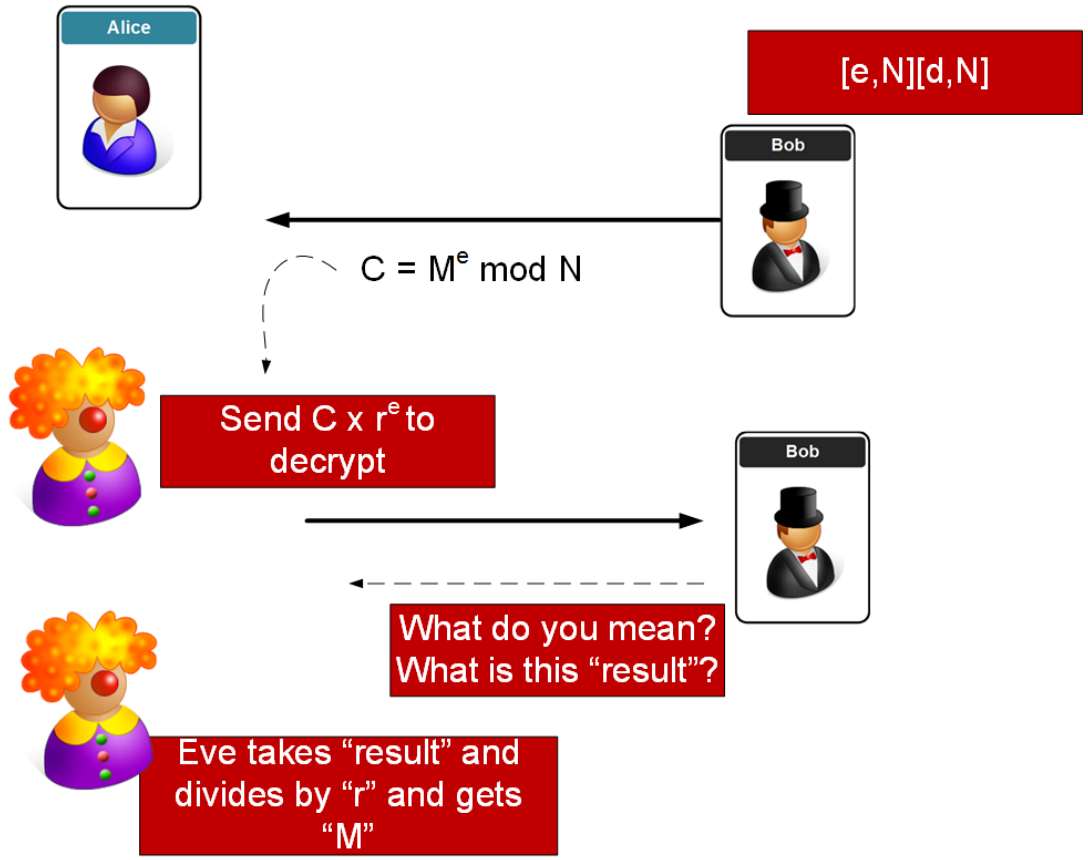
If Eve can determine the decrypted value for this cipher, she can determine the message as:

$$(C')^d = (C \times r^e)^d = (M^e \times r^e)^d = M^{e \times d} \times r^{e \times d} = M \times r$$

as $(M^e)^d(\mod N)$ must equal $M^1(\mod N)$

So Eve just takes the original cipher, and divides it by the random value (r).

Here is the method:



Coding

An outline of the code is:

```
e=79
d=1019
N=3337
r=3
M=8

cipher=M**e % N
print 'Initial cipher:\t',cipher
```

```
cipher_dash = cipher * (r**e) % N
print 'Eve gets Bob to decipher:\t',cipher_dash


decipher = cipher_dash **d % N

print 'Bob says that the result is wrong:',decipher

print 'Eve determines as:',decipher/r
```

Key calculation

Let's select:

```
P=47 Q=71
```

The calculation of n and PHI is:

```
n=P × Q = 13 × 11 = 3337
PHI = (p-1)(q-1) = 3220
```

We can select e as:

```
e = 79
```

Next we can calculate d from:

```
(79 × d) mod 3220 = 1 [Link]
d = 1019
Encryption key [3337,79]
Decryption key [3337,1019]
```

Then, with a message of 688, we get:

$$Cipher = (688)^{79} \mod 3337 = 1570$$

$$Decoded = (1570)^{1019} \mod 3337 = 688$$

Outline

Eve The Magician - Chosen Cipher Attack

Chosen Cipher Attack on RSA