Univariate Coppersmith Example

Nadia Heninger

UCSD

PCMI GSS Lecture 1

What's wrong with this RSA example?

```
message = Integer('squeamishossifrage',base=35)
N = random_prime(2^512)*random_prime(2^512)
c = message^3 % N
```

What’s wrong with this RSA example?

```
message = Integer(’squeamishossifrage’,base=35)
N = random_prime(2^512)*random_prime(2^512)
c = message^3 % N
```

```
sage: Integer(c^(1/3)).str(base=35)
’squeamishossifrage’
```

What’s wrong with this RSA example?

```
message = Integer(’squeamishossifrage’,base=35)
N = random_prime(2^512)*random_prime(2^512)
c = message^3 % N
```

```
sage: Integer(c^(1/3)).str(base=35)
’squeamishossifrage’
```

The message is too small.

This is why we use padding.

```
N = random_prime(2^150)*random_prime(2^150)
message = Integer(’thepasswordfortodayisswordfish’,base=35)
c = message^3 % N
```

```
N = random_prime(2^150)*random_prime(2^150)
message = Integer('thepasswordfortodayisswordfish',base=35)
c = message^3 % N
```

```
sage: int(c^(1/3))==message
False
```

```
N = random_prime(2^150)*random_prime(2^150)
message = Integer('thepasswordfortodayisswordfish',base=35)
c = message^3 % N
```

This is a stereotyped message. We might be able to guess the format.

```
N = random_prime(2^150)*random_prime(2^150)
message = Integer(’thepasswordfortodayisswordfish’,base=35)
c = message^3 % N
```

```
a = Integer(’thepasswordfortodayis000000000’,base=35)
```

```
N = random_prime(2^150)*random_prime(2^150)
message = Integer(’thepasswordfortodayisswordfish’,base=35)
c = message^3 % N
```

```
a = Integer(’thepasswordfortodayis000000000’,base=35)
```

```
X = Integer(’xxxxxxxxx’,base=35)
M = matrix([[X^3, 3*X^2*a, 3*X*a^2, a^3-c],
            [0,N*X^2,0,0],[0,0,N*X,0],[0,0,0,N]])
```

```
N = random_prime(2^150)*random_prime(2^150)
message = Integer(’thepasswordfortodayisswordfish’,base=35)
c = message^3 % N
```

```
a = Integer(’thepasswordfortodayis000000000’,base=35)

X = Integer(’xxxxxxxxx’,base=35)
M = matrix([[X^3, 3*X^2*a, 3*X*a^2, a^3-c],
            [0,N*X^2,0,0],[0,0,N*X,0],[0,0,0,N]])

B = M.LLL()
Q = B[0][0]*x^3/X^3+B[0][1]*x^2/X^2+B[0][2]*x/X+B[0][3]
```

```
N = random_prime(2^150)*random_prime(2^150)
message = Integer(’thepasswordfortodayisswordfish’,base=35)
c = message^3 % N
```

```
a = Integer(’thepasswordfortodayis000000000’,base=35)

X = Integer(’xxxxxxxxx’,base=35)
M = matrix([[X^3, 3*X^2*a, 3*X*a^2, a^3-c],
            [0,N*X^2,0,0],[0,0,N*X,0],[0,0,0,N]])

B = M.LLL()
Q = B[0][0]*x^3/X^3+B[0][1]*x^2/X^2+B[0][2]*x/X+B[0][3]

sage: Q.roots(ring=ZZ)[0][0].str(base=35)
’swordfish’
```