

Howgrave-Graham Example

Nadia Heninger

UCSD

PCMI GSS Lecture 2

```
p = random_prime(2^512); q = random_prime(2^512)
```

```
N = p*q
```

```
a = p - (p % 2^86)
```

```
p = random_prime(2^512); q = random_prime(2^512)
N = p*q
```

```
a = p - (p % 2^86)
```

```
sage: hex(a)
'a9759e8c9fba8c0ec3e637d1e26e7b88befeb03ac199d1190
76e3294d16ffcaef629e2937a03592895b29b0ac708e79830
4330240bc0000000000000000000'
```

Key recovery from partial information.

```
p = random_prime(2^512); q = random_prime(2^512)
```

```
N = p*q
```

```
a = p - (p % 2^86)
```

```
X = 2^86
```

```
M = matrix([[X^2, X*a, 0], [0, X, a], [0, 0, N]])
```

```
B = M.LLL()
```

```
p = random_prime(2^512); q = random_prime(2^512)
```

```
N = p*q
```

```
a = p - (p % 2^86)
```

```
X = 2^86
```

```
M = matrix([[X^2, X*a, 0], [0, X, a], [0, 0, N]])
```

```
B = M.LLL()
```

```
Q = B[0][0]*x^2/X^2+B[0][1]*x/X+B[0][2]
```

```
sage: a+Q.roots(ring=ZZ)[0][0] == p
```

```
True
```