>

MATH 243 -- Mathematical Structures
RSA Public-Key Encryption Example
October 31, November 1, 2017

Consider the RSA system with

$m = 11 \cdot 13 = 143$ (much too small to be a secure system, but OK for "hand" calculations!)

The public information would be the encryption exponent e and the number $m = 143$. We will use $e = 7$ so the encryption function is $f(x) = x^7 \bmod 143$.

Let's take the plaintext message "MEET AT DAWN" converted to numerical form in the simplest way (A = 0, B = 1, C = 2, etc.)

```
> plaintext := [12, 4, 4, 19, 0, 19, 3, 0, 22, 13];
```

$$plaintext := [12, 4, 4, 19, 0, 19, 3, 0, 22, 13] \quad (1)$$

We apply the encryption function to each number in the plaintext message like this:

```
> f := x→x^7 mod 143;
```

$$f := x \to x^7 \bmod 143 \quad (2)$$

```
> ciphertext := map(f, plaintext);
```

$$ciphertext := [12, 82, 82, 46, 0, 46, 42, 0, 22, 117] \quad (3)$$

>

The decryption exponent in this case is $d = 103$ since

```
> 7·103 mod (11-1)·(13-1);
```

$$1 \quad (4)$$

So to decrypt:

```
> g := x→ x^103 mod 143;
```

$$g := x \to x^{103} \bmod 143 \quad (5)$$

```
> decrypt := map(g, ciphertext);
```

$$decrypt := [12, 4, 4, 19, 0, 19, 3, 0, 22, 13] \quad (6)$$

which recovers the original plaintext(!)