

# MATH 110: Class 12

## September 1: Cryptography

---

### Cryptography

1. **Cryptography.** Cryptography is the practice of hiding information, often through mathematical means. Translating a message into a “secret code” so that someone else who knows the same code can decrypt it is a typical example.
2. **Public-key cryptography.** In public-key cryptography, sometimes called *asymmetric cryptography*, each user has two *cryptographic keys*, that is, pieces of information (for our purpose, numbers) that control the encryption/decryption processes.
  - A user’s *public key* is available publicly, i.e., everyone has access to it. Anyone can encrypt a message using the public key. In particular, one need not have access to secret information to encrypt a message!
  - A user’s *private key* is typically known only to the user. The private key can be used to decrypt a message encrypted using the public key, but it should be difficult to recover the private key from the public key, meaning that only the someone with the private key can decrypt a message encrypted using the public key.
  - Thus, encryption with the public key is a so-called *one-way function*: It is easy to compute but difficult to invert without additional information, hence it is difficult to read an encrypted message without the private key.
  - The two main applications of public-key cryptography are
    - (a) public key encryption and
    - (b) digital signatures.
3. **The RSA public-key cryptosystem.** The RSA (Rivest–Shamir–Adleman) cryptosystem is a common public-key cryptosystem. We introduce it with a running example.

- **Choosing keys.**

- (a) Choose 2 distinct prime numbers,  $p$  and  $q$ —keep these secret! (In applications these are typically very large, say, around  $2^{128}$ , but smaller primes work fine for our purposes.)

EXAMPLE.

Take  $p = 11$  and  $q = 13$ .

- (b) Calculate the *modulus*,

$$n = pq.$$

$$n = pq = 11 \cdot 13 = 143.$$

- (c) Calculate Euler’s totient  $\phi(n)$  of  $n = pq$ : Recall from yesterday that since  $\phi$  is multiplicative, it satisfies

$$\phi(n) = \phi(pq) = \phi(p)\phi(q) = (p-1)(q-1).$$

*Remark: This is the original formulation of the RSA algorithm. Nowadays, Carmichael’s totient function,  $\lambda$  is used instead and often results in faster computations; for  $n = pq$  as above,  $\lambda(n) = \text{lcm}(p-1, q-1)$ .*

$$\phi(143) = \phi(11)\phi(13) = 10 \cdot 12 = 120.$$

*Instead using Carmichael’s totient function gives  $\lambda(143) = 60$ .*

- (d) Choose an integer *exponent*  $e$  such that  $1 < e < \phi(n)$  coprime to  $\phi(n)$ . (Common values include 3, 5, 35, 65537; these numbers are common in part because they have a small Hamming weight, which allows for more efficient encryption.)

Since  $\phi(187) = 160$  is not divisible by 3, we may as well take.

$$e = 3.$$

- (e) Compute a *private key*  $d$  such that  $de = 1 \pmod{\phi(n)}$ , i.e., such that  $de = 1 + k\phi(n)$  for some integer  $x$ .

Since  $1 + 2 \cdot 160 = 321$  is divisible by  $e = 3$ , we may take  $d = \frac{321}{3} = 107$ .

*If we instead use Carmichael's totient function, so that we look for a  $d$  satisfying  $de = 1 \pmod{\lambda(n)}$ , that is,  $3d = 1 \pmod{80}$ , we could take  $d = 27$ , which would make later computations easier.*

- (f) The public key is the pair  $(n, e)$ , consisting of the modulus and the exponent, and, as above, the private key is  $d$ .

- The public key is  $(187, 3)$ .
- The private key is 107.

- **Encryption.** Given a numerical *plaintext* message  $m$ , we use the public key  $(n, e)$  to compute a *ciphertext*  $c$ ; this is our secret message.

- The ciphertext is:

$$c = m^e \pmod{n}.$$

By definition the sender knows  $m$ , and  $e$  and  $n$  are public.

Suppose that we wish to send a 2-digit message, say,  $m = 42$  (a text message can be converted to/from a numerical value by any means we like). We need to compute  $m^e \pmod{n} = 42^3 \pmod{187}$ .

This looks like a big computation, but we can break it up as follows:

- \* First, compute

$$\begin{aligned} 42^2 \pmod{187} &\equiv 1764 \pmod{187} \\ &\equiv 81 \pmod{187} \end{aligned}$$

- \* Multiplying again by 42 gives

$$\begin{aligned} 42^3 &\equiv 42^2 \cdot 42 \pmod{187} \\ &\equiv 81 \cdot 42 \pmod{187} \\ &\equiv 3402 \pmod{187} \\ &\equiv 36 \pmod{187} \end{aligned}$$

**The square-and-multiply method.** More generally, to compute  $a^b \pmod{n}$ , we can successively compute  $a \pmod{n}$ ,  $a^2 \pmod{n}$ ,  $a^4 \pmod{n}$ , etc. and then write  $b$  as a sum of powers of 2, namely, 1, 2, 4, etc; that way, we never need to compute using a number larger than  $n^2$ . This is the *square-and-multiply method*.

- **Decryption.** If someone has encrypted a message using our public key  $(n, e)$  and sent us the resulting ciphertext  $c$ , we can decrypt the ciphertext, i.e., recover the original message, by computing

$$m = c^d \pmod{n}.$$

The modulus  $n$  is publicly known, and we should assume that ciphertext  $c$  is public, because it may be intercepted. But only we can decrypt the message, because only we know the private key,  $d$ .

- Why does this work? Because

$$\begin{aligned} c^d \pmod{n} &\equiv (m^e)^d \pmod{n} \\ &\equiv m^{de} \pmod{n} \\ &\equiv m^{1+\phi(n)} \pmod{n} \\ &\equiv m \cdot m^{\phi(n)} \pmod{n} \\ &\equiv m \pmod{n} \end{aligned}$$

The last equivalence follows from Euler's Theorem:  $m^{\phi(n)} \equiv 1 \pmod{n}$ .  
 Notice that the message  $m$  must be shorter than the modulus  $n$  to recover it!

To decrypt the message, we compute

$$36^{107} \pmod{187}.$$

This is a more formidable computation before. One option is to use an online calculator like the Power Mod Calculator. But we can also still carry out the computation manually using square-and-multiply method:

$$\begin{aligned} 36^1 &\equiv 36 \pmod{187} \\ 36^2 &\equiv 36^2 \pmod{187} \equiv 174 \pmod{187} \\ 36^4 &\equiv 174^2 \pmod{187} \equiv 169 \pmod{187} \\ 36^8 &\equiv 169^2 \pmod{187} \equiv 137 \pmod{187} \\ 36^{16} &\equiv 137^2 \pmod{187} \equiv 69 \pmod{187} \\ 36^{32} &\equiv 69^2 \pmod{187} \equiv 86 \pmod{187} \\ 36^{64} &\equiv 86^2 \pmod{187} \equiv 103 \pmod{187} \end{aligned}$$

Decomposing 107 as a sum of powers of 2 (recall that this is the same as converting 107 to binary!) gives  $107 = 64 + 32 + 8 + 2 + 1$ , so

$$\begin{aligned} 36^{107} \pmod{187} &\equiv 36^{64} \cdot 36^{32} \cdot 36^8 \cdot 36^2 \cdot 36^1 \pmod{187} \\ &\equiv 103 \cdot 86 \cdot 137 \cdot 174 \cdot 36 \pmod{187} \\ &\equiv 42 \pmod{187} \end{aligned}$$

We have recovered our secret message from the ciphertext! (Note that the number of terms in this final multiplication is equal to the Hamming weight of  $d$ .)

*If we instead we use Carmichael's totient function, we need only compute  $36^{27} \pmod{187}$ , and again we find  $36^{27} \pmod{187} = 42 \pmod{187}$ ; computing using the square-and-multiply method would require only computing powers up to  $36^{16}$ .*

#### ACTIVITY (Encrypting and decrypting a message with the RSA algorithm).

- Generate a public key  $(n, e)$  and corresponding private key  $d$ .
- Give your public key,  $(n, e)$ , to a neighbor, and receive a public key  $(n', e')$  from them.
- Choose a message  $m' < n'$ , compute the ciphertext  $c'$  using your neighbor's public key, and then give them  $c'$ .
- Use your private key  $d$  and ciphertext  $c$  to decrypt the message  $m$  that your neighbor chose; verify with them that  $m$  is indeed the message they encrypted.