

RSA Scribe Notes

Introduction to Discrete Structures

Kathryn Breedlove

October 6, 2026

1 Context

This lecture applies the number theory from earlier in the course (modular arithmetic, GCDs, inverses, Euler's theorem) to a real-world problem: sending secrets over a public channel. RSA, named for Rivest, Shamir and Adleman (1977), is one of the first and most widely used public-key systems. It is a good example of how “pure” discrete math becomes the basis of secure web traffic, messaging and online payments.

2 The Big Picture

RSA lets two people communicate privately without ever having to share a secret key in advance.

Alice and Bob want to talk without anyone else hearing. In the old model they both hold a key to the same lockbox, which means they first had to agree on a key. Public-key cryptography removes that step:

- **Public key**: published for everyone. Anyone can use it to scramble (encrypt) a message.
- **Private key**: kept secret by the receiver. Only it can unscramble (decrypt) the message.
- **Plaintext** is the original message m ; **ciphertext** is the scrambled version c .

Here Alice owns the key pair and Bob sends her a message. Security rests on a math fact: multiplying two big primes is easy, but recovering them from their product is believed to be very hard.

3 Math Toolkit

RSA is built from five ideas: modular arithmetic, the GCD and Bézout's identity, modular inverses, Euler's theorem, and fast exponentiation.

3.1 Modular arithmetic

$a \equiv b \pmod{N}$ means $N \mid (b - a)$. Every number is equivalent to exactly one remainder in $\mathbb{Z}_N = \{0, 1, \dots, N - 1\}$. You may reduce before or after adding or multiplying:

$$(a+b) \bmod N = ((a \bmod N) + (b \bmod N)) \bmod N, \quad ab \bmod N = ((a \bmod N)(b \bmod N)) \bmod N.$$

Example: $(14 + 3) \bmod 5 = 2$, and $(14 \bmod 5) + (3 \bmod 5) = 4 + 3 = 7 \equiv 2 \pmod{5}$.

Why it holds: write $a = q_1N + r_1$ and $b = q_2N + r_2$. Then $a + b = (q_1 + q_2)N + (r_1 + r_2)$ and $ab = (q_1q_2N + q_1r_2 + q_2r_1)N + r_1r_2$, so only the remainders matter.

3.2 GCD and Bézout's identity

For any a and N there are integers x, y with

$$ax + Ny = \gcd(a, N).$$

The extended Euclidean algorithm finds x and y . Reducing mod N gives $ax \equiv \gcd(a, N) \pmod{N}$.

3.3 Multiplicative inverses

a has an inverse mod N if there is an x with $ax \equiv 1 \pmod{N}$. This happens exactly when $\gcd(a, N) = 1$. In that case Bézout gives $ax + Ny = 1$, so x is the inverse of a .

Modulus	Inverses ($a \rightarrow a^{-1}$)	No inverse
5	$1 \rightarrow 1, 2 \rightarrow 3, 3 \rightarrow 2, 4 \rightarrow 4$	none (5 is prime)
10	$1 \rightarrow 1, 3 \rightarrow 7, 7 \rightarrow 3, 9 \rightarrow 9$	0, 2, 4, 5, 6, 8

Check: $3 \cdot 7 = 21 \equiv 1$ and $9 \cdot 9 = 81 \equiv 1 \pmod{10}$.

3.4 Euler's totient and Euler's theorem

Definition. $\mathbb{Z}_N^*$ is the set of elements of $\mathbb{Z}_N$ coprime to N , and $\varphi(N) = |\mathbb{Z}_N^*|$.

$\mathbb{Z}_N^*$ is closed under multiplication, and multiplying by a fixed $a \in \mathbb{Z}_N^*$ just shuffles the set (the map $x \mapsto ax$ is one-to-one), which is why every element has an inverse.

- $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$, so $\varphi(10) = 4$.
- For a prime p : $\varphi(p) = p - 1$.
- For distinct primes p, q : count everything, remove the multiples of p (q of them) and of q (p of them), and add back pq itself, which was removed twice:

$$\varphi(pq) = pq - p - q + 1 = (p - 1)(q - 1).$$

Theorem (Euler). If $\gcd(a, N) = 1$, then $a^{\varphi(N)} \equiv 1 \pmod{N}$.

Example, $N = 10$: $3^4 = 81 \equiv 1$, $7^4 = 2401 \equiv 1$, $9^4 = 6561 \equiv 1 \pmod{10}$.

Proof. Multiply every element of $\mathbb{Z}_N^*$ by a . The result is the same set in a different order, so the two products agree: $a^{\varphi(N)} P \equiv P \pmod{N}$, where P is the product of all elements. Since P is invertible, $a^{\varphi(N)} \equiv 1$. $\square$

Fermat's little theorem is the prime case: if p is prime and $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.

3.5 Fast exponentiation

Computing $a^n \pmod{N}$ by repeated squaring takes about $\log n$ steps instead of n . This is what makes RSA practical with numbers hundreds of digits long.

4 The RSA Algorithm

Alice picks two large primes, publishes $N = pq$ and e , and keeps d secret. Bob encrypts with (N, e) ; Alice decrypts with d . In practice N is about 2048 bits (roughly 600 decimal digits), and the message is a number $m \in \{0, 1, \dots, N - 1\}$.

Key generation (Alice)

1. Pick two large primes p and q .
2. Compute $N = pq$ and $\varphi(N) = (p - 1)(q - 1)$.
3. Find e with $\gcd(e, \varphi(N)) = 1$.
4. **Public key** $= (N, e)$.
5. **Secret key** $d = e^{-1} \bmod \varphi(N)$, found with the extended Euclidean algorithm, so $ed \equiv 1 \pmod{\varphi(N)}$.

Encryption (Bob)

Given a message m and Alice's public key (N, e) :

$$c = m^e \bmod N.$$

Decryption (Alice)

Using her secret key d :

$$m = c^d \bmod N.$$

Both steps use fast exponentiation, so they are quick even for 2048-bit numbers. An eavesdropper sees N , e and c , but computing d requires $\varphi(N)$, which requires factoring N into p and q .

5 Why Decryption Works

Decrypting gives back m because d and e are inverses mod $\varphi(N)$, and Euler's theorem makes the extra powers of m disappear.

Since $ed \equiv 1 \pmod{\varphi(N)}$, there is an integer k with $ed = 1 + k\varphi(N)$. If $\gcd(m, N) = 1$, Euler's theorem gives

$$c^d \equiv (m^e)^d = m^{ed} = m^{1+k\varphi(N)} = m \cdot (m^{\varphi(N)})^k \equiv m \cdot 1^k = m \pmod{N}.$$

So Alice recovers m exactly. This argument assumes m is coprime to N ; with huge primes almost every message is, and RSA also works for the rare exceptions (usually shown with Fermat's little theorem mod p and mod q , which goes beyond these notes).

6 Worked Example

With $p = 11$ and $q = 17$, Bob's message 42 becomes 15 and Alice's key $d = 23$ turns it back into 42.

Step	Who	Computation
Pick primes	Alice	$p = 11, q = 17$
Compute N	Alice	$11 \cdot 17 = 187$
Compute $\varphi(N)$	Alice	$(11 - 1)(17 - 1) = 10 \cdot 16 = 160$
Choose e	Alice	$\gcd(7, 160) = 1$, so $e = 7$
Find d	Alice	$7 \cdot 23 = 161 = 1 + 160$, so $d = 23$
Publish	Alice	public key $(N, e) = (187, 7)$
Encrypt	Bob	$42^7 \bmod 187 = 15$
Decrypt	Alice	$15^{23} \bmod 187 = 42$

7 Cheat Sheet

Item	Value	Who knows it
p, q	large primes	Alice only
N	pq	everyone
$\varphi(N)$	$(p - 1)(q - 1)$	Alice only
e	$\gcd(e, \varphi(N)) = 1$	everyone
d	$e^{-1} \bmod \varphi(N)$	Alice only
Encrypt	$c = m^e \bmod N$	Bob
Decrypt	$m = c^d \bmod N$	Alice

- An inverse mod N exists exactly when $\gcd(a, N) = 1$.
- Euler: $\gcd(a, N) = 1 \Rightarrow a^{\varphi(N)} \equiv 1 \pmod{N}$.
- Security relies on the difficulty of factoring N .

8 Practice Questions

1. Find the multiplicative inverse of 5 modulo 12. Then explain why 4 has no inverse modulo 12.
2. Compute $\varphi(15)$. Verify Euler's theorem for $a = 2$ and $N = 15$.
3. Let $p = 5$ and $q = 11$. Find N and $\varphi(N)$, choose $e = 3$, and compute the secret key d .
4. Using the keys from question 3, encrypt $m = 4$, then show how Alice decrypts the ciphertext.
5. Why must $\gcd(e, \varphi(N)) = 1$? Why can an eavesdropper who knows N , e and c not easily recover m ?