Definition 14. Euler's phi function $\phi(n)$ denotes the number of integers in $\{1, 2, ..., n\}$ that are relatively prime to n.

In other words, $\phi(n)$ counts how many residues are invertible modulo n.

If the prime factorization of n is $n = p_1^{k_1} \cdots p_r^{k_r}$, then $\phi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$.

Why is this true?

- Why is the formula "obvious" if $n = p^k$ is a prime power?
- On the other hand, for composite n, say $n = ab$, we have $\phi(ab) = \phi(a)\phi(b)$ if $\gcd(a, b) = 1$. This is a consequence of the Chinese remainder theorem. (Review if necessary!)

The above formula follows from combining these two observations. Can you fill in the details?

Example 15. Compute $\phi(100)$.

Solution. $\phi(100) = \phi(2^2 \cdot 5^2) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40$.

Example 16. (homework) Evaluate $\phi(2016)$ and $\phi(10^n)$.

Theorem 17. (Euler's theorem) If $n \geqslant 1$ and $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

More about this later!

Do review these basic number theory facts if you feel a bit rusty.

2 Historical examples of symmetric encryption

Alice wants to send a secret message to Bob.

What Alice sends will be transmitted through an unsecure medium (like the internet), meaning that others can read it. However, it is important to Alice and Bob that noone else can understand it.

The original message is referred to as the **plaintext** m. What Alice actually sends is called the **ciphertext** c (the encrypted message).

Symmetric encryption algorithms rely on a secret key k shared by Alice and Bob (but unknown to anyone else).

Our ultimate goal will be to secure messaging against both:

- eavesdropping (confidentiality)
- tampering (integrity/authenticity)

The symmetric encryption approach, by itself, cannot fully protect against tampering. For instance, an attacker can collect previously sent messages, resend them, or use them to replace new messages. (You could preface each message with something like a time stamp to address these issues. But that's getting ahead of ourselves; and there are better ways.)

Armin Straub
straub@southalabama.edu

2.1 Shift cipher

The alphabet for our messages will be $A, B, ..., Z$, which we will identify with $0, 1, ..., 25$.

So, for instance, C is identified with the number 2.

Example 18. (shift cipher) A key is an integer $k \in \{0, 1, ..., 25\}$. Encryption works character by character using

$$E_k: \quad x \mapsto x + k \pmod{26}$$

Obviously, the decryption D_k works as $x \mapsto x - k \pmod{26}$.

The **key space** is $\{0, 1, ..., 25\}$. It has size 26. [Well, $k = 0$ is a terrible key. Maybe we should exclude it.]

For instance. If $k = 1$, then the message $HELLO$ is encrypted as $IFMMP$.

If $k = 2$, then the message $HELLO$ is encrypted as $JGNNQ$.

Historic comment. Caesar encrypted some private messages with a shift cipher (typically using $k = 3$). The shift cipher is therefore also often called Caesar's cipher.

While completely insecure today, it was fairly secure at the time (with many of his enemies being illiterate).

Modern comment. Many message boards on the internet "encrypt" things like spoilers or solutions using a shift cipher with $k = 13$. This is called ROT13. What's special about the choice $k = 13$?

Solution. Since $-13 \equiv 13 \pmod{26}$, for ROT13, encryption and decryption are the same!

Example 19. (homework) Encrypt the message $SPOILER$ using ROT13. What happens if we encrypt it a second time?

Example 20. The challenge from Example 13 was encrypted using a shift cipher. The key space has size 26, so a brute-force attack results in immediate success: we find that $k = 2$ and that the plaintext is $GREETINGSSTRANGER$.

This is the worst kind of vulnerability: we successfully mounted a **ciphertext only attack**.

That is, just knowing the encrypted message, we were able to decrypt it (and discover the key that was used).

2.2 Vigenere cipher (vector shift cipher)

See Section 2.3 of our book for a full description of the Vigenere cipher.

This cipher was long believed by many (until early 20th) to be secure against ciphertext only attacks.

Example 21. Let us encrypt $HOLIDAY$ using a Vigenere cipher with key BAD (i.e. $1, 0, 3$).

	H	O	L	I	D	A	Y
$+$	B	A	D	B	A	D	B
$=$	I	O	O	J	D	D	Z

Hence, the ciphertext is $IOOJDDZ$.

Example 22. (homework) The message $QSYNGGI$ was encrypted by your friend Alice using a Vigenere cipher with the key USA. Decrypt it.

Example 23. (bonus challenge!) Eve, can you crack the following message?

$$UYGSQOYYFHGMFUA$$

Word on the street is that Alice was using the Vigenere cipher with a key of size 2.