Additive Cipher

ENCRYPTION

1. **Select a "key,"** a single number to be used encrypt a message with modular addition, mod 26.
2. **Use alphanumeric substitution** to change every letter in your message to its corresponding numeric value in modulus 26.
3. **Encrypt** the message by adding the key to each numeric value from alphanumeric substitution.
4. **Divide** each encrypted number by the modulus (26) and replace it with the resulting **remainder**.
5. **Use** alphanumeric substitution to rewrite each number by its corresponding letter.

DECRYPTION

1. **Use alphanumeric substitution** to change every letter in your message to its corresponding numeric value in modulus 26.
2. **Add** the (additive) inverse of the key to each numeric value from alphanumeric substitution.
3. **Add** the modulus (26) to each resulting value that is negative. Repeat until the value lies in the domain of mod 26.
4. **Use** alphanumeric substitution to rewrite each number by its corresponding letter

$$19 + 9 = 38 = 12 \; mod \; 26$$
$$9 + (-19) = -10 \; = \; 16 \; mod \; 26$$

ALPHANUMERIC SUBSTITUTION

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Modular Arithmetic

Modular arithmetic is the arithmetic of congruences, in which the number of available numerical quantities is limited by the **modulus** and includes only whole numbers. For example, there are 12 available numbers in a modulus 12 (**mod 12**) number system: **0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11**. Any mathematical operation in mod 12 that produces a result outside the available numbers "wraps" around to give a final answer in the modulus. This "wrapping" is executed by division (divisor: modulus; dividend: number to be "wrapped"), with the final answer being the resulting **remainder**.

Public Key Encryption

Modular arithmetic has been the basis for **public-key cryptographic systems** since their development in the 1970s. Historically, public-key cryptography utilizes large prime numbers and **modular exponentiation** for encryption to create factorization problems that are difficult (but not impossible) to solve for decryption. They are called **one-way functions** due to the computational complexity necessary for solution. Public-key cryptography uses a combination of public and private information between sender and receiver: the receiver provides a public-key for any sender to use for secure encryption using a specific public-key cryptographic algorithm, but keeps the private key for decryption using that same cryptographic algorithm.

NAVY NOTES

Data Integrity

Parity bits (mod 2) are used the check the accuracy of a string of binary code by ensuring that the number of bits in the string is correctly even or odd. ASCII letters (mod 2) have 7-bits, saving the 8th bit for a parity bit. **Check digits** are used in large data-entry systems to catch human errors in data entry, and are used throughout industry and commerce (ISBN and UPC codes are both mod 11). **Error-correcting codes** such as the Hamming Code (mod 2) can not only detect errors in binary code, but can also correct them to ensure data integrity during transmission. Error-correcting codes are the precursors of **hash functions**, an encryption technique to check for data tampering or interception during transmission.

ALPHANUMERIC SUBSTITUTION

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24