Introduction

Alex Shaffer

What is Cryptography?

- A collection of methods used to secure information.
  - Has a long history of being used to secure military information in wartime.
  - Helps protect transaction information online.
  - Can be used to secure stored data on a phone.

Important Terms

- Text that has not been encrypted or has been decrypted is called **plaintext**.
- Text that has been encrypted is called **ciphertext**.
- An **algorithm** is a set of instructions.
  - **Encryption** is an algorithm that takes plaintext and produces ciphertext.
  - **Decryption** is an algorithm that takes ciphertext and produces plaintext.

Sets

- Sets are just collections of elements. We will be most interested in sets of numbers and letters.
- A set of numbers will be denoted with curly brackets {}
  - $\mathbb{N}$ is the set of natural numbers. $\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$
    - Some people don't include 0, we will.
  - $\mathbb{Z}$ is the set of integers. $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$
  - $\mathbb{R}$ is the set of real numbers and include all integers and decimal values, and special numbers like π.

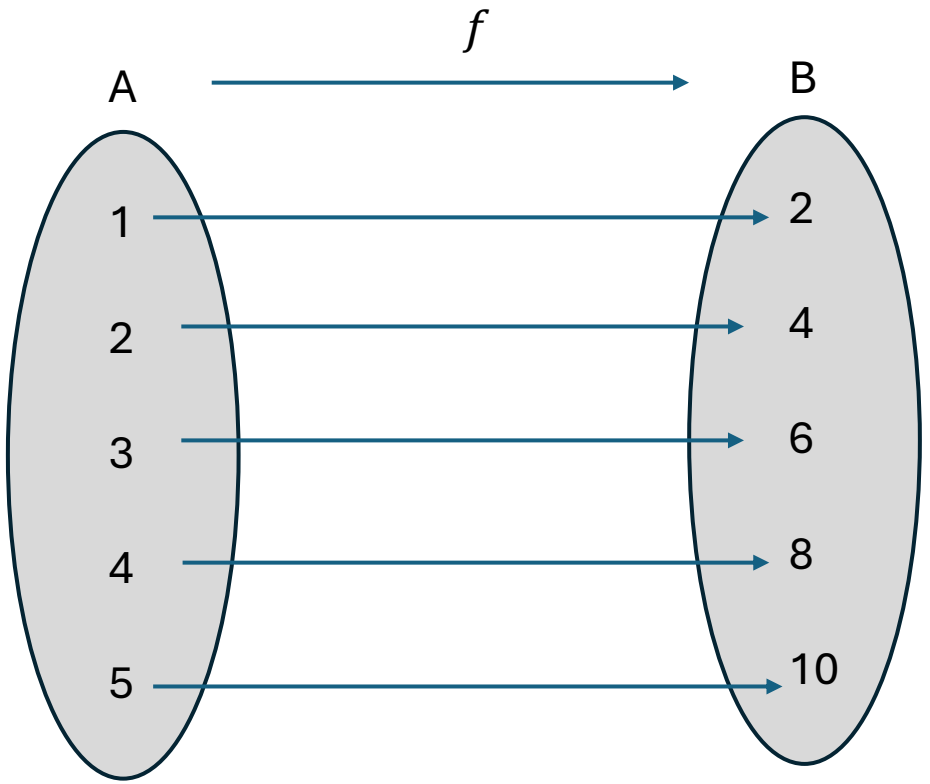
Functions

- A **function** is like a mathematical machine that takes in an input and produces an output.
  - It maps elements from one set to elements of another
- If A is some set and B is another set, we denote a function f mapping elements from A to elements of B as $f: A \to B$
- Example: $f: \mathbb{N} \to \mathbb{N}$, where $f(x) = x + 2$

x	0	1	2	3	4	5	6
$f(x)$	2	3	4	5	6	7	8

Functions

- $f: A \to B$



Representing Information

- Standard English alphabet may be represented as the integers 0 through 25 inclusive.
  - $a \rightarrow 0, b \rightarrow 1, c \rightarrow 2, \ldots, z \rightarrow 25$
  - "Hello world" → $8\ 5\ 12\ 12\ 15 \quad 23\ 15\ 18\ 12\ 4$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
U	V	W	X	Y	Z														
20	21	22	23	24	25														

Binary

- Binary representation useful in computer implementation of cryptography.
  - Each 0 or 1 is called a “bit”.
  - Right most bit is called least significant, left is most significant.

0	1	2	3	4	5	6	7	8	9
0	1	10	11	100	101	110	111	1000	1001

ASCII TABLE

Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char
0	0	[NULL]	32	20	[SPACE]	64	40	@	96	60	`
1	1	[START OF HEADING]	33	21	!	65	41	A	97	61	a
2	2	[START OF TEXT]	34	22	"	66	42	B	98	62	b
3	3	[END OF TEXT]	35	23	#	67	43	C	99	63	c
4	4	[END OF TRANSMISSION]	36	24	$	68	44	D	100	64	d
5	5	[ENQUIRY]	37	25	%	69	45	E	101	65	e
6	6	[ACKNOWLEDGE]	38	26	&	70	46	F	102	66	f
7	7	[BELL]	39	27	'	71	47	G	103	67	g
8	8	[BACKSPACE]	40	28	(	72	48	H	104	68	h
9	9	[HORIZONTAL TAB]	41	29	)	73	49	I	105	69	i
10	A	[LINE FEED]	42	2A	*	74	4A	J	106	6A	j
11	B	[VERTICAL TAB]	43	2B	+	75	4B	K	107	6B	k
12	C	[FORM FEED]	44	2C	,	76	4C	L	108	6C	l
13	D	[CARRIAGE RETURN]	45	2D	-	77	4D	M	109	6D	m
14	E	[SHIFT OUT]	46	2E	.	78	4E	N	110	6E	n
15	F	[SHIFT IN]	47	2F	/	79	4F	O	111	6F	o
16	10	[DATA LINK ESCAPE]	48	30	0	80	50	P	112	70	p
17	11	[DEVICE CONTROL 1]	49	31	1	81	51	Q	113	71	q
18	12	[DEVICE CONTROL 2]	50	32	2	82	52	R	114	72	r
19	13	[DEVICE CONTROL 3]	51	33	3	83	53	S	115	73	s
20	14	[DEVICE CONTROL 4]	52	34	4	84	54	T	116	74	t
21	15	[NEGATIVE ACKNOWLEDGE]	53	35	5	85	55	U	117	75	u
22	16	[SYNCHRONOUS IDLE]	54	36	6	86	56	V	118	76	v
23	17	[END OF TRANS. BLOCK]	55	37	7	87	57	W	119	77	w
24	18	[CANCEL]	56	38	8	88	58	X	120	78	x
25	19	[END OF MEDIUM]	57	39	9	89	59	Y	121	79	y
26	1A	[SUBSTITUTE]	58	3A	:	90	5A	Z	122	7A	z
27	1B	[ESCAPE]	59	3B	;	91	5B	[	123	7B	{
28	1C	[FILE SEPARATOR]	60	3C	<	92	5C	\	124	7C	|
29	1D	[GROUP SEPARATOR]	61	3D	=	93	5D	]	125	7D	}
30	1E	[RECORD SEPARATOR]	62	3E	>	94	5E	^	126	7E	~
31	1F	[UNIT SEPARATOR]	63	3F	?	95	5F	_	127	7F	[DEL]

Modular Arithmetic

- Sometimes it is useful to constrain numbers to a certain set.
- $a \equiv b \ (mod\ n)$ is said “a is congruent to b modulo n”
  - Two numbers are equivalent modulo n if they have the same remainder when divided by n.
- Examples:
  - $1 \equiv 3 \ (mod\ 2)$
  - $15 \equiv 20 \ (mod\ 5)$
  - $26 \equiv 0 \ (mod\ 26)$
  - $5 \equiv 31 \ (mod\ 26)$

Modular Arithmetic

- For any number a where $a > n$ there is some number $b < n$ where $a \equiv b \ (mod\ n)$
  - $2 \equiv 7 \equiv 12 \equiv 17 \ (mod\ 5)$
    - 2 is the is the number less that 5 here that all of the others are equivalent to
  - The set of numbers $\{0, 1, 2, \dots, n - 1\}$ is called the **canonical complete residue system modulo n**

Caeser Cipher

- Sometimes called a shift cipher.
- Encryption key k is some number 0 through 25.
  - For a plaintext letter p written as a number, the ciphertext letter $c = p + k \ (mod\ 26)$
  - Example: $k = 1$,

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U

U	V	W	X	Y	Z
V	W	X	Y	Z	A

  - “Hello world” → “jgnnq yqtnf”