Block Ciphers

Alex Shaffer

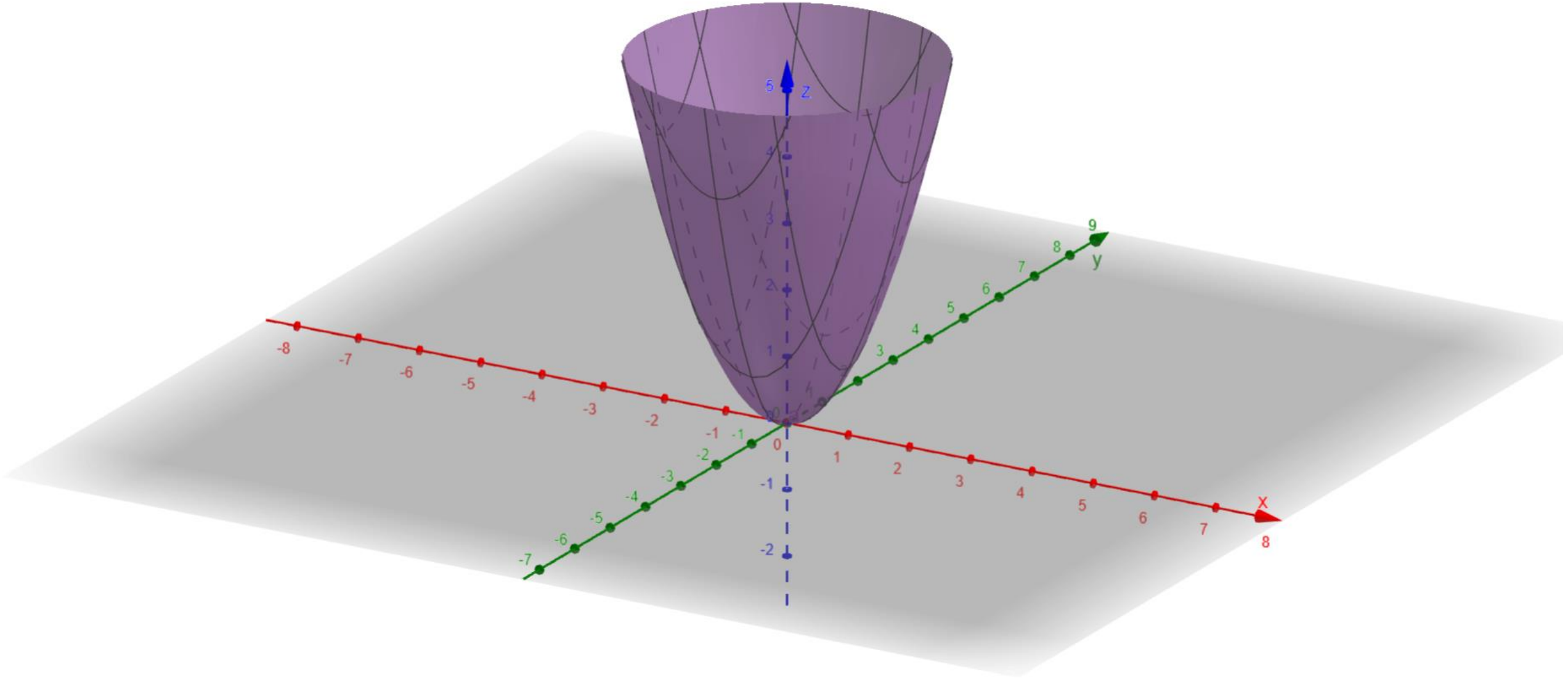
More on Sets

- We will be dealing with the following set throughout the following section.
  - $\{0, 1\}$
  - This set is the just the numbers 0, and 1. Simple!
  - This is a representation of a “bit” of information
- If we have 2 bits, we can represent it in the following way
  - $\{0, 1\}^2 = \{0, 1\} \times \{0, 1\} = \{(0, 0),\ (0, 1),\ (1, 0), (1, 1)\}$
  - This is called a Cartesian Product
- k different bits is represented by $\{0, 1\}^k$
  - Each element from this cartesian product is a string of k bits

More on Functions

- So far we have seen function of only one variable. But this need not always be the case.
  - As an example, let us say $f\colon \mathbb{R}^2 \to \mathbb{R}$ which is a function from pairs of real numbers to the real numbers.
  - An example of such a function is $f(x, y) = x^2 + y^2$

Image of the Function



Block Ciphers

- A slightly more abstract description of encryption.
  - Encryption is a function of a key K of bit length k, and a plaintext message P of bit length n.
    - We want a choice of n and k, such that k|n.
  - $E(K, P)$: $\{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$
  - Decryption is still just the inverse of encryption.
  - $D(K, C)$: $\{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$
    - Where $D(K, C) = E^{-1}(K, P)$

What does this mean?

- Of the plaintext string P of size n and a key of size k where k divides n, we apply the encryption method to P in blocks of size k.

Caesar Cipher

- The Caesar cipher is a block cipher.
  - Each letter is a number 0 through 25.
  - These numbers may be converted to binary, where each letter is 5 bit number. (more commonly, you may see characters represented by 8-bits of using ascii)

0	1	2	3	4	5	6	7	8	9
00000	00001	00010	00011	00100	00101	00110	00111	01000	01001
10	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**
01010	01011	01100	01101	01110	01111	10000	10001	10010	10011
20	**21**	**22**	**23**	**24**	**25**				
10100	10101	10110	10111	11000	11001				

Caesar Cipher

- The key to a Caesar cipher is just another number 0 through 25.
- The size of the key is $k = 5$ bits
- The Caesar cipher encrypts in 5-bit blocks, adding the key to the letter and taking that modulo 26.

XOR Operator

- xor is short for “exclusionary or”
- When you have two bits, b_1 and b_2, you could ask “is b_1 or b_2 equal to 1”.
  - If both are 1 and this statement is true, then this is the “inclusive” or.
  - If both are 1 and this is not true, then this is the “exclusive” or.

XOR Operator

- We will write the the binary xor operator as follows.
  - $xor \rightarrow \oplus$ in the same way addition $\rightarrow +$
  - For two binary bits $b_1 \; and \; b_2$, there we can write their xor as $b_1 \oplus b_2$

b_1	b_2	$b_1 \oplus b_2$
0	0	0
0	1	1
1	0	1
1	1	0

XOR Cipher

- An xor cipher is an iterated block cipher in the same way a Caesar ciphjer was.
- You have a key of k bits, and plaintext of n bits.
- You xor bits from the plaintext and the key together to get the cipher text.
- To decrypt you just repeat the same process. It is its own inverse (called and involution)

XOR Cipher Example

- Let us use the 8-bit key: 10101010
- Using the ascii encoding of chatacters, we have that:
  - $Word = 01110111\ 01101111\ 01110010\ 01100100$
- Encryption:

Plaintext	01110111	01101111	01110010	01100100
Key	10101010	10101010	10101010	10101010
Ciphertext	11011101	11000101	11011000	11001110

XOR decryption

- To decrypt we will just use the same key and the xor operator

Ciphertext	11011101	11000101	11011000	11001110
Key	10101010	10101010	10101010	10101010
Plaintext	01110111	01101111	01110010	01100100

- This is exactly the same as the plaintext we put in.