Crypto\_challenge

**1. For the following cipher (ASCII coding), determine the decoded string: %68%61%69%72**

Additional information:

a (%61) b (%62) c (%63) d (%64) e (%65) f (%66) g (%67) h (%68) i (%69) j (%6A) k (%6B)

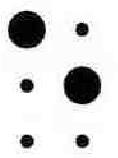
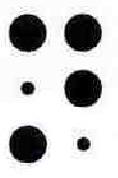
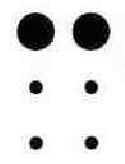
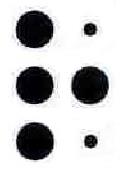
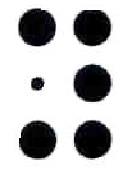
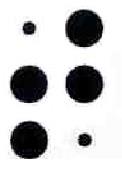
l (%6C) m (%6D) n (%6E) o (%6F) p (%70) q (%71) r (%72) s (%73) t (%74) u (%75) v (%76)

w (%77) x (%78) y (%79) z (%80) SPACE (%20)

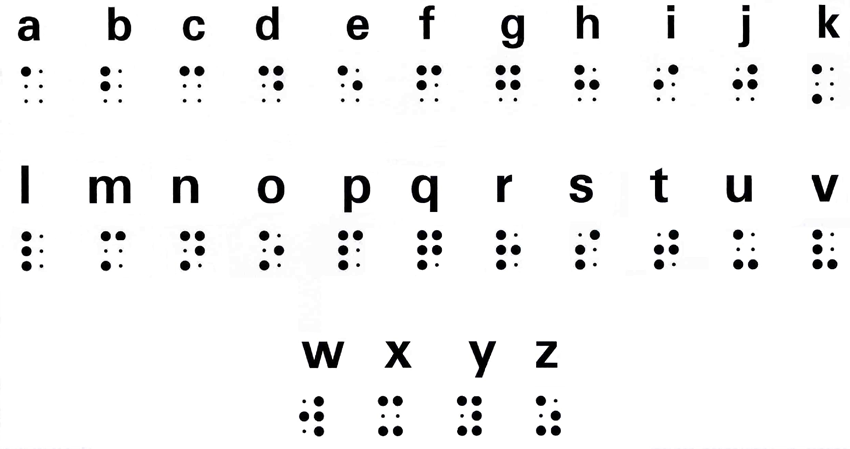
**Answer**:

|  |  |  |  |
| --- | --- | --- | --- |
| %68 | %61 | %69 | %72 |
| H | A | I | R |
| **hair** | | | |

**2. Solve this Braille cipher:**

**      **

Additional information:



**Answer:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| **Encrypt** | | | | | | |

**3. Solve the gold bug cipher to recover the plaintext: \*‡(]5:**

Additional information:

The Gold-Bug cipher was included in a short story by Edgar Allan Poe and which was published in 1843. It tells the tale of William Legrand and how he was bitten by a gold-colored bug. The mapping is:

abcdefghijklmnopqrstuvwxyz

52-†81346,709\*‡.$();?¶]¢:[

In the book he writes:

Here Legrand, having re-heated the parchment, submitted it to my inspection. The following characters were rudely traced, in a red tint, between the death's-head and the goat:

53‡‡†305))6\*;4826)4‡.)4‡);806\*;48†8¶60))85;1‡(;:‡\*8†83(88)5\*†;

46(;88\*96\*?;8)\*‡(;485);5\*†2:\*‡(;4956\*2(5\*—4)8¶8\*;4069285);)6†8

)4‡‡;1(‡9;48081;8:8‡1;48†85;4)485†528806\*81(‡9;48;(88;4(‡?

34;48)4‡;161;:188;‡?;

This is translated as:

5 - A

3‡‡† - good

305)) - glass

6\* - in

;48 - the

Ans:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| \* | **‡** | ( | ] | 5 | : |
| N | O | R | W | A | Y |
| **Norway** | | | | | |

**4. What is the plain text for the following Bacon cipher: BAAAB AABBB AABAA ABABA AABAB**

Ans:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **BAAAB** | **AABBB** | **AABAA** | **ABABA** | **AABAB** |
| S | H | E | L | F |
| **shelf** | | | | |

**5. What is the plain text for the Dvorak cipher of: IPAOO**

Additional information:

Plain: abcdefghijklmnopqrstuvwxyz

Cipher: axje.uidchtnmbrl'poygk,qf;

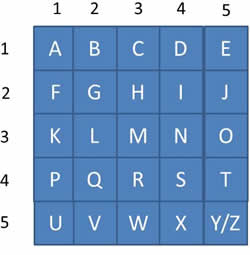
Ans:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| I | P | A | O | O |
| G | R | A | S | S |
| **grass** | | | | |

**6. What is the plain text for the following tap cipher: . .. .. .... ... ..... ... ... . ..... .... ..... .... ... .. .... . ...**

Additional information:

The tap cipher uses a Polybius mapping, and where we tap (.) out the row and then tap the column count:



For example:

.... ..... . . .... .... .... ..... . .....

T A S T E

Ans:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| . .. | .. …. | … ….. | … … | . ….. | …. ….. | …. … | .. …. | . … |
| G | I | O | M | E | T | R | I | C |
| **giometric** | | | | | | | | |

**7. With a Caeser cipher, if we use either a 1 letter, 2 letter or 3 letter shift (as defined below), which one is the plaintext for: RJCUG**

Additional information:

For a 1 letter shift:

abcdefghijklmnopqrstuvwxyz

BCDEFGHIJKLMNOPQRSTUVWXYZA

for two shifts:

abcdefghijklmnopqrstuvwxyz

CDEFGHIJKLMNOPQRSTUVWXYZAB

and three shifts:

abcdefghijklmnopqrstuvwxyz

DEFGHIJKLMNOPQRSTUVWXYZABC

Ans:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| shift value | R | J | C | U | G |
| 1 | Q | I | B | T | F |
| 2 | P | H | A | S | E |
| 3 | O | G | Z | R | D |
| Solution | **Phase** | | | | |

**8. For the following Morse code, what is the plaintext: (···) (·— —·) (·) (·—) (·—·)**

Ans:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **(···)** | **(·— —·)** | **(·)** | **(·—)** | **(·—·)** |
| S | P | E | A | R |
| **Spear** | | | | |

**9. The Diffie Hellman method allows Bob and Alice to exchange values and end up with the same result. Calculate the shared value for: G=337, N=1399, x=5, y=4**

Additional information:

In Diffie-Hellman, Bob and Alice agree on G (a generator) and N (a prime number), and then Bob picks a random value of x, and Alice picks a random value of y:

Bob (x) Alice (y)

b=G^x mod N

a=G^y mod N

Bob sends Alice the value of b Alice sends Bob the value of a

Key=a^x mod N

Key=b^y modN

Ans:

**Key Value is 1,267**

**10. With this OTP we EX-OR the message with a one-time key (see below). Calculate the hex values for the following cipher: Word: simulator Key: slippy**

Additional information:

If we take a message of "hello" and a key of "goodbye", we get:

hello 01101000 01100101 01101100 01101100 01101111

goodbye 01100111 01101111 01101111 01100100 01100010 01111001 01100101

Now if we EX-OR them we get:

01101000 01100101 01101100 01101100 01101111

01100111 01101111 01101111 01100100 01100010

--------------------------------------------

00001111 00001010 00000011 00001000 00001101

0 f 0 a 0 3 0 8 0 d

So the result is 0f0a03080d

Binary values

To help you, here are a list of binary values:

a chr(97) 01100001

b chr(98) 01100010

c chr(99) 01100011

d chr(100) 01100100

e chr(101) 01100101

f chr(102) 01100110

g chr(103) 01100111

h chr(104) 01101000

i chr(105) 01101001

j chr(106) 01101010

k chr(107) 01101011

l chr(108) 01101100

m chr(109) 01101101

n chr(110) 01101110

o chr(111) 01101111

p chr(112) 01110000

q chr(113) 01110001

r chr(114) 01110010

s chr(115) 01110011

t chr(116) 01110100

u chr(117) 01110101

v chr(118) 01110110

w chr(119) 01110111

x chr(120) 01111000

y chr(121) 01111001

z chr(122) 01111010

With hex values, we take four bits at a time and convert the values:

0000 0

0001 1

0010 2

0011 3

0100 4

0101 5

0110 6

0111 7

1000 8

1001 9

1010 A

1011 B

1100 C

1101 D

1110 E

1111 F

Ans:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Word 1 | Binary | Word 2 | Binary | EX OR | HEX |
| S | 01110011 | S | 01110011 | 00000000 | 00 |
| I | 01101001 | L | 01101100 | 00000101 | 05 |
| M | 01101101 | I | 01101001 | 00000100 | 04 |
| U | 01110101 | P | 01110000 | 00000101 | 05 |
| L | 01101100 | P | 01110000 | 00011100 | 1C |
| A | 01100001 | Y | 01111001 | 00011000 | 18 |
| T | 01110100 | S | 01110011 | 00000111 | 07 |
| O | 01101111 | L | 01101100 | 00000011 | 03 |
| R | 01110010 | I | 01101001 | 00011011 | 1B |

**Final Answer: 000504051C1807031B**

**11. RSA Encryption parameters. Public key: [e,N].**

e: 65537

N: 696026718829707141234015255193382147

Cipher: 6255639640170097520001174621866023

We are using 60-bit primes

Can you find the value of the message?

Answer:

Using <https://www.alpertron.com.ar/ECM.HTM> we calculated p and q:

P: 670302131471996423

Q: 1038377600413143589

(p-1) \* (q-1) = 696026718829707139525335523308242136

Using WolfarmAlpha, we calculated ‘d’: 627132425147538132489602249894741873

Graphical user interface, text, application, email

Description automatically generated

Again, WolfarmAlpha to calculate m using decryption: F(c,d) = c^d mod n

(<https://www.wolframalpha.com/widgets/view.jsp?id=570e7445d8bdb334c7128de82b81fc13>)

Graphical user interface, text, application, email

Description automatically generated

Result: 1403