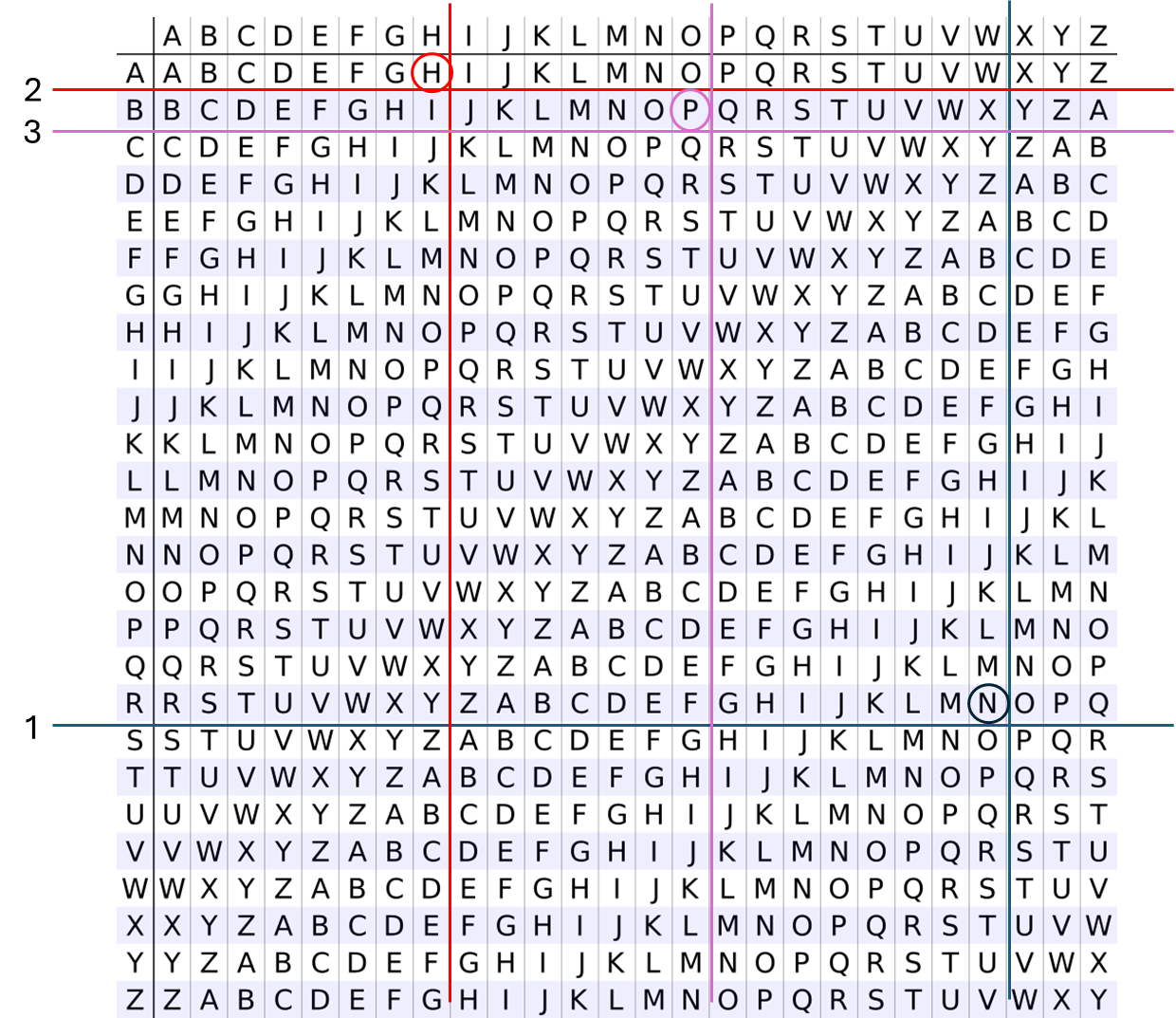
A screenshot of a computer

Description automatically generatedTask 1:

Task 2:

Plaint text: Who is the queen of hearts?

Key: rabbithole  
  
Cipher Text: Nhp ja mos byveo pn alocxj?

Task 3:

P: 13

Q: 29

E: 17

C: 4

After switching C: 270

This tells us that this operation is equivalent to decrypting the initial plaintext with this original e and d values.

Task 4:

H2 (second-preimage resistance) prevents an attacker from taking a document that you had previously signed and later claiming that you signed a different document.

H3 (collision resistance) prevents an attacker from getting you to sign a specific document and then later claiming that you signed a different document.

Addition: because I’m not sure that it’s clear what the difference from the description above (the book really doesn’t do a great job at describing H2 in particular), the main difference is that in H2, the attacker does not get to pick/create the original signed document, whereas in H3, the original signed document is chosen/created by the attacker.

Task 5:

A block cipher process plain text in fixed-size chunks (called blocks). Each block is encrypted with a fixed transformation dependent on the key. Its main properties are block length and key length. Additionally, when a block does not have the requisite number of characters, filler characters are added. Keys are generated by creating a random string of a specific length.

A stream cipher encrypts data one bit or character at a time. These ciphers turn a fixed-size secret key into an arbitrary length keystream. The next plaintext bit or character is then encrypted with a position-varying transformation dependent on the input key. Keys are generated by turning a fixed length symmetric key into an arbitrary-length secret keystream.