*Some interesting points from QCAA worth mentioning*:

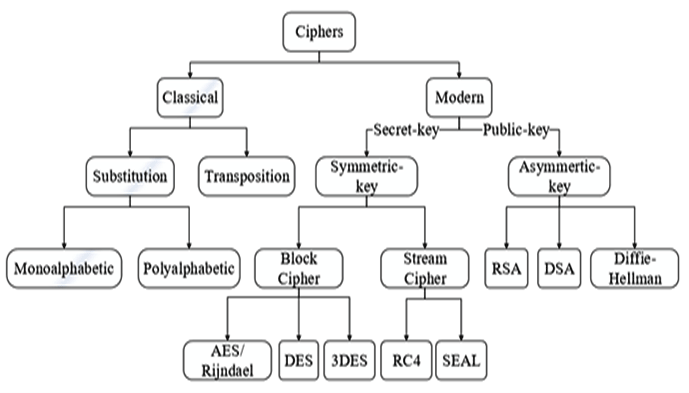
|  |
| --- |
| “Multiple choice items can be constructed in range of different ways although they will always consist of:   * stem (the question being asked), * key (the correct answer) and * distractors (which are incorrect but plausible).”   “Marks are allocated according to the evidence available. **Marks aren’t deducted — evidence is rewarded**.”  “The QCAA sample and mock external assessments were designed to demonstrate options in what an assessment will look like. There will clearly be similarities and differences. The external assessments in 2020 and beyond will exist somewhere on a continuum with these two instruments. This is a deliberate and purposeful decision made to **minimise predictability** but **allow transparency** about what may be coming.” |

****

*Questions – complete the following*:

1. Encryption or authentication strategies (complete the yellow unfilled squares):

|  |  |  |
| --- | --- | --- |
| Acronym | Full Name | Defining features or brief explanation of how it works *in your own words*: |
| DES |  |  |
| 3DES |  |  |
| RSA |  |  |
| AES |  |  |
|  | Blowfish |  |
|  | Twofish |  |
|  | Feistel block cipher | <https://www.tutorialspoint.com/cryptography/feistel_block_cipher.htm>  “Feistel Cipher is not a specific scheme of block cipher. It is a design model from which many different block ciphers are derived. DES is just one example of a Feistel Cipher. A cryptographic system based on Feistel cipher structure uses the same algorithm for both encryption and decryption. The encryption process uses the Feistel structure consisting **multiple rounds** of processing of the plaintext, each round consisting of a “*substitution*” step followed by a *permutation* step.” |



1. Briefly explain the difference between the following terms from the diagram from the previous question:

|  |  |
| --- | --- |
| Term | Meaning or brief description (*in your own words*) |
| Substitution |  |
| Transposition |  |
| Monoalphabetic |  |
| Polyalphabetic |  |
| Symmetric |  |
| Asymmetric |  |
| Block cipher |  |

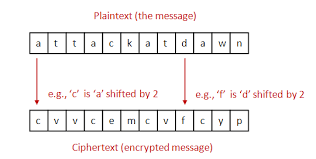
1. Fill in the missing parts of this table of Data exchange languages/formats:

|  |  |  |
| --- | --- | --- |
| Acronym | Full name | Characteristics or features of its syntax: |
| JSON |  |  |
| CSV |  |  |
| XML |  |  |

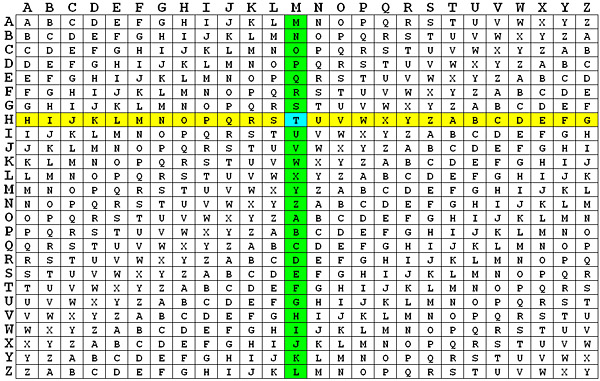
1. Complete the table of Network transmission methods or protocols:

|  |  |  |
| --- | --- | --- |
| Acronym | Full name | Definition, characteristics, or explanation of how it works: |
| HTTP |  |  |
| HTTPS |  |  |
| FTP |  |  |
| VPN |  |  |
| IP |  |  |
| TCP |  | *Consider timeliness vs guarantee of delivery*? |
| UDP |  | *Consider timeliness vs guarantee of delivery*? |

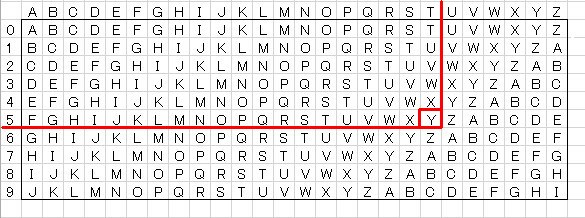
1. In the following encryption algorithm, all letters are shifted by the same value (+2). What type of cipher is this commonly known as?



1. In the following encryption algorithm, I am encrypting the plain text “M” with the key “H”. What type of cipher is this commonly known as?



1. In the following encryption algorithm, I am encrypting the plain text “T” with the key 5. What type of cipher is this commonly known as?

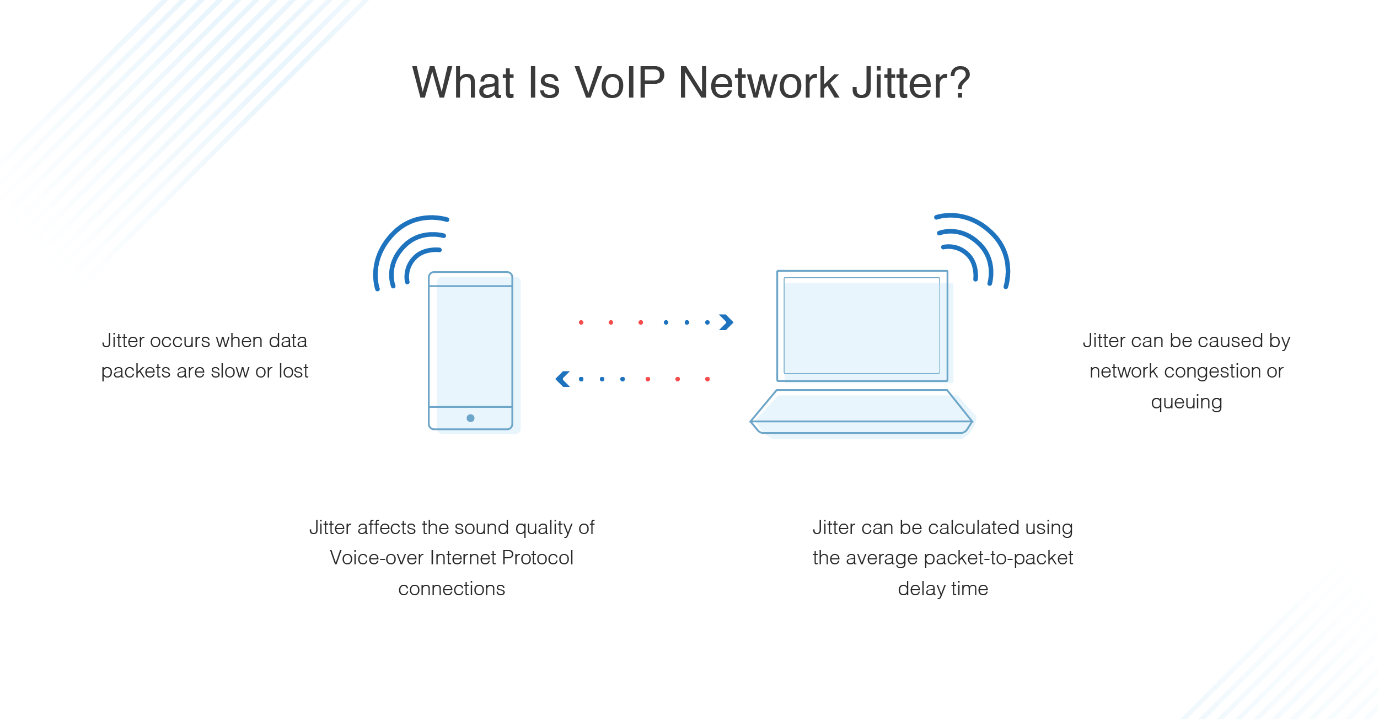


1. The following example uses the “One-Time Pad” method of encryption:

|  |  |  |  |
| --- | --- | --- | --- |
| Plaintext: | Y | A | Y |
| OTP Key: | A | B | C |
| Ciphertext: |  |  |  |

* 1. Calculate the cipher text in the table above
  2. One is it claimed that the One-Time Pad method is such a strong form of encryption that it “cannot be cracked”?
  3. [extension] There is a sample implementation of this algorithm in Python here: <https://digisoln.com/skulpt/python/demo/onetimepad_cipher.py>. Can you code the decryption algorithm for this in Python, that takes a cipher text and a OTP key as an input, then decodes the output?

1. Would latency (delay) and jitter cause the same problems for streaming and broadcasting data packet, as it does for VoIP? (see following diagram).



1. Briefly explain the principles of REST. What makes a REST-ful API?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

1. Explain how data compression1, encryption2 and *hashing* are used in the storage and transfer of data. Use the definitions (from above) and examples where possible to illustrate your points:

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

*From the Digital Solutions syllabus glossary*:

|  |
| --- |
| 1 **compression**: a process of encoding information using fewer bits, i.e. 0 or 1, than an original representation, to reduce file size, typically using mathematical formulas to remove repeated data, combine related data or simplify data, e.g. a line segment can be represented by the position of the end points instead of every dot on it;  common examples include:   * .zip files, which can contain one or more files or folders that have been compressed * .jpg files in digital photography are produced by processing complete (lossless) data from a camera’s sensor through compressing (looking for redundant/unnecessary data) into a smaller file size * .mp3 files for audio, which compress an original audio source to reduce the file size significantly but still sound like an exact copy of the original |
| 2 **encryption**: a process in cryptography of encoding (converting) data, using mathematical formulas, into a form that only an intended recipient can decode, often including a personal digital signature, e.g. when connecting to an online banking or shopping website, typically on login, a secure communication is set up based on encryption provided at the website, and this will be represented by a https://URL and a lock symbol on the user’s internet browser |