**Exercise 1: Designing an Algorithm**

Your first task is to implement an algorithm in pseudocode to encrypt a message. Pens and paper are at the front of the lab if you need them.

The encryption algorithm you should implement is described below and is based on the Rip-van-Winkle cypher,

[https://en.wikipedia.org/wiki/Rip\_van\_Winkle\_cipher URL](https://en.wikipedia.org/wiki/Rip_van_Winkle_cipher%20URL)

To encrypt a message, the sender must pick a "TimeSlot" at random (see table below) and for each letter in the message offset that letter by the number in the corresponding index of the letter in the "TimeSlot". Once the message has been encrypted the sender must send the TimeSlot number, wait for an acknowledgement and then send the encrypted message.

HINT: if the letter being encrypted is "a", the index of the letter in the message is 4, the number in the corresponding index of TimeSlot 1 is 9, the encrypted letter a would be "j".

Below are the set of 5 TimeSlot which your algorithm should randomly select from.

| **Index** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | **16** | **17** | **18** | **19** | **20** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| TimeSlot 1: | 6 | 8 | 3 | 9 | 9 | 4 | 6 | 2 | 4 | 8 | 1 | 9 | 7 | 3 | 1 | 6 | 5 | 3 | 7 | 1 |
| TimeSlot 2: | 3 | 7 | 1 | 5 | 2 | 9 | 1 | 3 | 9 | 4 | 7 | 1 | 2 | 1 | 2 | 5 | 1 | 9 | 5 | 2 |
| TimeSlot 3: | 1 | 1 | 4 | 4 | 5 | 7 | 8 | 5 | 3 | 1 | 6 | 4 | 8 | 7 | 1 | 6 | 3 | 6 | 4 | 6 |
| TimeSlot 4: | 7 | 5 | 6 | 9 | 8 | 4 | 4 | 7 | 1 | 9 | 9 | 2 | 3 | 4 | 7 | 8 | 2 | 7 | 8 | 4 |
| TimeSlot 5: | 4 | 9 | 8 | 1 | 3 | 2 | 2 | 1 | 7 | 6 | 8 | 8 | 9 | 6 | 3 | 9 | 5 | 8 | 1 | 3 |