# Computer chatter

## Tablets of Stone: Extension

The following describes an extension to CS Unplugged's Tablets of Stone, and provides printable templates for variations that introduce a security layer to the activity.

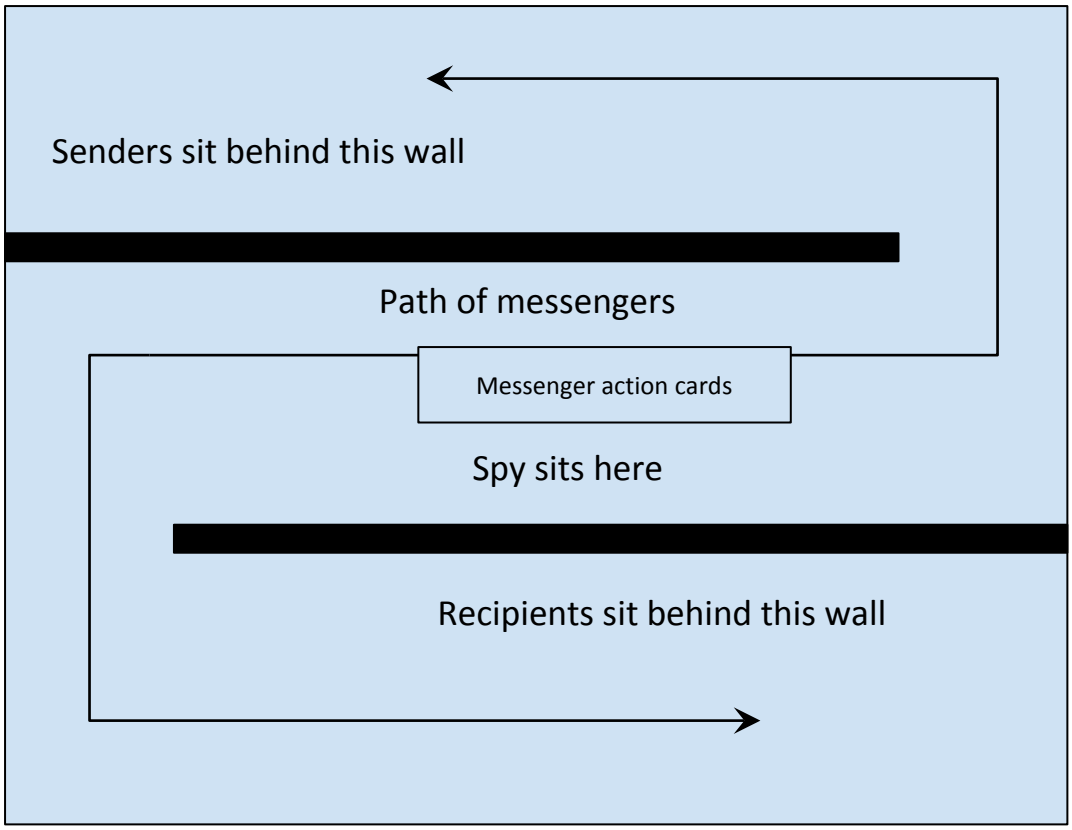
### 'Secure' Tablets of Stone

The activity works in a similar way to the CS Unplugged Tablets of Stone activity, but with the following additions:

- a new role: **the spy** (it may be best that the teacher is the spy, since you don't want students to know that the spy is in the game)
- two copies of a new action card per messenger deck: **Deliver this message to the spy**
- rule changes for the spy.

**Preparation**

With the addition of the spy, it is imperative that the senders and recipients are in different locations and are not visible to one another. They also cannot see the spy, and the spy should be in a location where messengers must pass by them to move between the communicating parties. A good layout for this would be to use adjacent rooms, with an external hallway between them. Alternatively, you may be able to use barriers in your classroom to create a similar setup. The diagram below shows one such arrangement.




© 2016 Education Services Australia Ltd, unless otherwise indicated.
Creative Commons BY 4.0 licence, unless otherwise indicated.

DIGITAL TECHNOLOGIES HUB

Prepare the activity as before, this time adding the new action cards into each messenger deck. In addition to the other setup rules, you will need to:

- provide the spy with a set of tablets (they may need quite a few)
- ensure the spy has a piece of paper to write things down.

**Playing the game**

The game proceeds as normal; however, this time when a messenger draws the 'Deliver this message to the spy' action, the messenger will deliver the message to the spy instead of the intended recipient. The spy then records the message they have intercepted on their piece of paper, with the details of the sender, recipient and message contents. They then choose to do one of the following:

- they can give the message back to the messenger, who then delivers it as normal.
- they can rewrite the message, changing its contents, then have the messenger deliver that to the recipient instead.

At **no time** should the messenger indicate to either the sender or recipient that the spy has seen the message.

As students add rules to the game to counter some of the problems that arise (the original activity explains some of these, and the kinds of solutions that students might come up with), you should add new actions for the spy that make it increasingly difficult for messages to get through. Some examples of these might be:

- when students have added a number that indicates the order of messages being sent, the spy could change that number but leave the rest of the message intact
- when students add an acknowledgement message to the process, have the spy spoof the acknowledgement so that the sender thinks it was received at the other end
- give the spy the power to look at every message that travels between two students once the action card is drawn
- allow the spy to look at every message at all times.

What students should begin to realise is that they need to share some information between themselves that will allow them to determine whether or not their message has been tampered with, as well as knowing whether it was received at the other end (the emphasis of the activity as written). One solution might be the introduction of a secret key that both partners share beforehand, which they then apply to each message and check before they acknowledge it has been received. If that key is not present in the message, then it is deemed to have been tampered with. The key could be a sequence of numbers that must appear in a specific order and that is not part of the message. (For example, both the numbers 2 and 4 must appear in the message in that order, but in any position. Those numbers are then ignored when working out the message contents. If a 2 or 4 is being sent, then the numbers must be repeated in a pattern that ensure the integrity of the message remains).

The challenge for the spy, then, is to try to work out what key is being used between the partners, which would allow them to read the message!

© 2016 Education Services Australia Ltd, unless otherwise indicated.
Creative Commons BY 4.0 licence, unless otherwise indicated.

**What's it all about?**

This variation introduces the concept of a 'man-in-the-middle' (MITM) attack, where a third party manages to intercept the communication between two other parties and either reads the messages being sent or alters their contents. If we consider this in terms of the transfer of data across a network, some of the more obvious implications of such an attack include:

- capturing sensitive data such as credit card numbers, which can then be used by the third party
- intentionally changing the message being sent between two parties – the attacker could direct someone to a different location for an intended meeting, which could have dire consequences.

The fact that MITM attacks can occur also introduces the need for some kind of encryption technique that not only ensures that the data is intact, but also that it cannot be read by someone who intercepts the packets. That way, if a MITM attack is successful, the data that is captured is not in a form that is usable. Cryptographic protocols and techniques, such as the Diffie-Hellman key exchange, provide the basis for more advanced techniques such as RSA public-key encryption used in modern communications.

If the techniques used to prevent MITM attacks are not strong enough, or the encryption used can be broken, then that technique cannot be used as the basis for secure, reliable communication in networks. The spy in our game is effectively a cyber-terrorist. They are intercepting messages and attempting to read their contents by looking for a key that reveals the messages' contents.

© 2016 Education Services Australia Ltd, unless otherwise indicated.
Creative Commons BY 4.0 licence, unless otherwise indicated.