Cryptography in the classroom

Public keys & Anonymity Lesson Plan

Level:	Aimed at S1-S2 Level (Suitable for S1-S5)
Estimated time:	10mins + 10min Activity
Materials Needed:	Public Keys & Anonymity Video, Public Keys Activity handout
	for each student, Coins for each group (for flipping)

Learning Outcomes: This lesson aims to:

- Inform the student about the steps in public key communications.

- Introduce the idea of intractable mathematics.

- Introduce the idea of anonymity and instruct the students on how to perform the 3DC protocol.

Lesson outline:

1. **Ask the students this question prior to watching the video :**
   "How would you tell someone a secret if they were on the other side of the room and everyone could hear them?"

   - A correct answer would mention encrypting the message before it's sent. Follow this answer up with another *rhetorical* question **"What if they didn't know the key before you started talking?"**. Rhetorical as that is exactly public key encryption.

2. **Show the "Public keys & Anonymity" Video to the class**

3. **Do activity 4**

   - Split the students into groups of 3. If there are mismatched numbers then make either one or two extended groups that do 4DC, The process is the same but just requires an 6 coin flips so everyone see's 3 shared coin flips - one for each other member of the group.

   - The 3DC protocol requires the use of XOR which is a concept that isn't covered at this level, using XOR is straightforward but still requires that the students write down their working.

   - For each group assign either : one person to act as the bill payer or have the bill payer be the teacher (GCHQ). Make note of this as it'll be needed to verify at the end. This can be done by playing heads down thumbs up and putting the students thumbs down if they are the one to "pay".

   - Once the students have finished have them call out their answer and reveal who the payee is.

     – If any group gets the incorrect answer follow their written working to show them were they went wrong.