THE UNIVERSITY *of* EDINBURGH

School of Informatics, Computing in the Classroom

Cryptography in the classroom

Public Keys & Anonymity Activity Sheet

Estimated time: 10mins

Activities:

1. We are going to be trying the 3DC protocol you just learnt about in the video.

   Follow the steps below :

   (a) Wait to be split into groups and assigned as player A, B, C (or D if in a group of 4)

   (b) The teacher will then ask you to put your heads on the table and put your thumbs up, once everyone's heads are down they might put down your thumbs - this means you are the payer! Don't tell anyone if you are or aren't the payer!

   (c) In your group flip a coin between each of the players (without letting the other player see it) and write down a 0 if it was heads or a 1 if it was tails in the outcome column of the table on the below (you will only need to fill out all 3 rows if you are in a group of 4).

Your Player Letter	Other Players Letter	**Outcome of coin flip**

   (d) Now take the outcome of both coin flips and find the XOR value of both of them. (In the table on the next page, x_1 would be the outcome of the first coin flip, x_2 is the outcome of the other coin flip) If you **are not** the payer then write down the

XOR value in the announcement box on the next page, if you **are** the payer then write down the *opposite* of the XOR value in the announcement box (If the value is 0 write 1, if it's 1 write 0, Use the table in part e) if you are in a group of 4).

x_1	x_2	x_1 **XOR** x_2
0	0	0
0	1	1
1	1	0
1	0	1

Announcement:	

(e) Show the other players in your group the number you wrote down in the announcement box (don't show them the other side of page!). Use the table below to find out who paid, if the outcome of the XOR of x_1, x_2, x_3 (player A, B and C's announcements) is 0 then the teacher paid if it's 1 then someone in the group paid! Put your hand up to see if you got it correct (if you are in a group of 4 take the result from the table below and use it as x_1 in the table above and x_2 will be player D's announcement).

x_1	x_2	x_3	x_1 **XOR** x_2 **XOR** x_3
0	0	0	0
0	0	1	1
0	1	1	0
1	1	1	1
1	1	0	0
1	0	0	1
1	1	0	0
0	1	0	1

Someone in group paid: □	**Teacher paid:** □