

How to flip a coin over e-mail?

Source: <http://sci.tech-archive.net/Archive/sci.math/2004-06/3670.html>

From: Jon Haugsand (jonhaug_at_ifi.uio.no)

Date: 06/17/04

Date: 17 Jun 2004 07:32:02 +0200

I have a real practical problem where I am going to place several people in the same number of rooms. However, the rooms are of different quality so the actual room any person get is done by random. There are som preconditions, so I can list all acceptable outcomes and the problem is to find some way to choose randomly between these outcomes.

How can I do this when all I have is e-mail communication between the participants?

My own solution is to make a file where I denumerate each outcome and shuffle them randomly. I pad this file with some secret random numbers at the end, and I send a cryptographic hash (md5) to all participants. I then ask the others for a number between 1 and N and this number will point to the actual outcome. I then send them the file such that all of them can check that I did not make this file after I got the number drawn.

However, this method requires that my friends have trust in the md5 cryptographic hash. Of course, they should, but I cannot demand such knowledge.

Any other method?

--

Jon Haugsand

Dept. of Informatics, Univ. of Oslo, Norway, <mailto:jonhaug@ifi.uio.no>

<http://www.ifi.uio.no/~jonhaug/>, Phone: +47 22 85 24 92