Some Observations on Reusing One-Time Pads within Dice Codings

Sebastian Pape
Databases and Interactive Systems Research Group
University of Kassel

In [D08] a Visual Cryptography System for internet banking based on Dice Codings was presented. In this system each user has a key-transparency, working as a One-Time Pad, which allows him to decrypt the ciphertext. Key-transparency, ciphertext and plaintext consist of ten segments each with nine points. Decryption is done pointwise. Points of the key-transparency are linked by a 'NOT XOR' function with their respective ciphertext’s counterparts and decrypt to a 'point' or 'no point' plaintext. Since each segment consists of nine 'points' or 'no points' digits from '0' to '9' can be represented by a plaintext segment.

If the key-transparency is used multiple times, we show that conclusions about it can be drawn. More precisely, the scope of key-transparencies can be reduced to the one used and its inverse. Our attack makes use of the fact, that each plaintext has to consist of all digits from '0' to '9'. Thus, plaintexts which include the same digit twice are invalid. Therefore, we are able to exclude key-transparencies which would decrypt to an invalid plaintext.

Since two segments can be attacked independently from the remaining eight segments, our proof of concept code only attacks two segments. 20 000 iterations suggest that 70 (90) key-transparencies are sufficient for our attack in more than 60 (95) percent. Since the proof of concept code does not make use of all information included in the observed ciphertexts, we claim that several improvements are possible.

Statistical observations show that the Visual Cryptography System presented in [D08] can be advanced by adding redundant segments. In the original system more than 18 percent of the possible plaintexts contain the same digit twice and, thus, are invalid. By adding two redundant segments it is possible to reduce the number of invalid keys below one percent. This countermeasure reduces the amount of information given per ciphertext sufficiently to counter our attack.

In the talk we discuss our attack and its improvements and we propose a simple improvement of the Visual Cryptography System presented in [D08], which counters our attack.

References