COMP6441 Tutorial 2: Houdini and 'Margy'

Youhan Cheery

March 20, 2017

1 Objectives

1. Public to everyone to verify.
2. Medium cannot be able to manipulate the message.
3. Easy enough to check and hard enough to fake.
4. Need to know if message has been compromised.

Are the endpoints secure? Even if Houdini were on the other side, does he necessarily want to give the mediums the satisfaction of disproving his work while he was alive? Does Bess want to tell the truth and thus tarnish Houdini's name in the case that he is actually speaking through the medium?

2 The Protocol

Houdini tells the public C which is a large product of two primes, A and B. He tells his wife B and the ISBN of a random book he wants to use before death. Houdini dies. His spirit tells the medium the ISBN and A encrypted by the contents of the book the ISBN points to. The wife knows the ISBN and no one else does. She can then decrypt the message. She can prove to the public that she did, because she can show them the ISBN.

Problem: other ISBNs could encrypt to the same thing.