Merkle’s puzzles

Ralph Merkle suggested a cryptosystem which is reminiscent of public- key cryptology already in 1974. It allows for two parties to agree on a shared key by communicating in the open.

Alice generates a number of puzzles and sends them to Bob. Bob solves one of them and tells Alice which one, he solved, but such that nobody else will know which puzzle he solved. In each puzzle there is a key. Using crypto terms this scenario could be as follows. Alice constructs N different cryptosystems and the plaintexts

”message i, symmetric key Ki”

for i from 1 to N . She encrypts the texts using the N different cryptosystems with the respective keys Ki and publishes all ciphertexts. Bob performs a brute-force attack on an arbitrary cipher j and finds the value of Kj. He sends to Alice the text ”message j” in cleartext. After this, Alice and Bob share the key Kj. If it is assumed that it takes M operations to brute-force one cipher, then Alice does N operations, Bob M operations but an attackter on this cryptosystem will require about MN operations. For example, with N = M, one gets a cryptosystem with N^2 (quadratic) security.

The N different cryptosystems could be the same, for example, the AES but used with different keys. To make it useful in practice, one could fix some (most) of the bits of an AES key.

To be of any use in practice the maximum values for M and N are probably around 2^25. If these numbers were much bigger, the time to exchange a key would be too high for it to be a practical key-exchange protocol. With N = M = 2^25 one gets a cryptosystem with a level of 2^50 security which is much more than 2^25. Still, this security level is not high enough for what is normally required today.

As far as I know, Merkle’s puzzles were never considered attractive enough for real-world applications. But it is noticeable that Merkles ideas were conceived before the publication of the epic public-key paper by Diffie and Hellman.

LRK. 2019.