## The Unbreakable Cipher

John Young jya at pipeline.com Wed Sep 25 10:11:33 EDT 2013

- Previous message: [tor-talk] Tor Weekly News September 25th, 2013
- Messages sorted by: <a>[ date ]</a> [ thread ] [ subject ] [ author ]

NSA Technical Journal published "The Unbreakable Cipher" in Spring 1961.

http://www.nsa.gov/public\_info/\_files/tech\_journals/The\_Unbreakable\_Cipher.pdf

Excerpts:

[Quote]

David Kahn, "Lyen Otuu Wllwgh WI Etjown" pp. 71, 83, 84, 86, 88 and 90 of the New York Times Magazine November 13, 1960 says that an unbreakable cipher system can be made from one time key "that is absolutely random and never repeats." ...

For each cipher system there is an upper bound to the amount of traffic it can protect against cryptanalytic attack. What is "cryptanalytic attack"? It is a process applied to cipher text in order to extract information, especially information contained in the messages and intended to be kept secret. If some of the information is gotten by other means and this results in more being extracted from the cipher, this is (at least partially) a successful attack. If certain phrases can be recognized when they are present, this is successful cryptanalysis. If a priori probabilities on possible contents are altered by examination of the cipher, this is cryptanalytic progress. If in making trial decipherments it is possible to pick out the correct one then cryptanalysis is successful. ...

Another example is that of Mr. Kahn, one-time key. Here the limit is quite clear; it is the amount of key on hand. The key arrives in finite "messages," so there is only a finite amount on hand at anyone time, and this limits the amount of traffic which can be sent securely. Of course another shipment of key raises this bound, but technically another cipher system is now in effect, for by my definition a cipher system is a message. A sequence of messages is a sequence of cipher systems, related perhaps, but not the same. ...

[Answer to the question:] "Does there exist an unbreakable cipher" would be this, "Every cipher is breakable, given enough traffic, and every cipher is unbreakable, if the traffic volume is restricted enough."

[End quote]

Previous message: [tor-talk] Tor Weekly News — September 25th, 2013

• Messages sorted by: [date] [thread] [subject] [author]

More information about the cypherpunks mailing list