Cryptology ePrint Archive: Report 2013/184

The Vernam cipher is robust to small deviations from randomness

Boris Ryabko

Abstract: The Vernam cipher (or one-time pad) has played an important rule in cryptography because it is a perfect secrecy system. For example, if an English text (presented in binary system) $X_1 X_2 ... $ is enciphered according to the formula $Z_i = (X_i + Y_i) \mod 2 $, where $Y_1 Y_2 ...$ is a key sequence generated by the Bernoulli source with equal probabilities of 0 and 1, anyone who knows $Z_1 Z_2 ... $ has no information about $X_1 X_2 ... $ without the knowledge of the key $Y_1 Y_2 ...$. (The best strategy is to guess $X_1 X_2 ... $ not paying attention to $Z_1 Z_2 ... $.) But what should one say about secrecy of an analogous method where the key sequence $Y_1 Y_2 ...$ is generated by the Bernoulli source with a small bias, say, $P(0) = 0.49, $ $ P(1) = 0.51$? To the best of our knowledge, there are no theoretical estimates for the secrecy of such a system, as well as for the general case where $X_1 X_2 ... $ (the plaintext) and key sequence are described by stationary ergodic processes. We consider the running-key ciphers where the plaintext and the key are generated by stationary ergodic sources and show how to estimate the secrecy of such systems. In particular, it is shown that, in a certain sense, the Vernam cipher is robust to small deviations from randomness.

Category / Keywords: running-key cipher, Vernam cipher, Shannon entropy, unconditional secrecy

Date: received 9 Mar 2013, last revised 2 Apr 2013

Contact author: boris at ryabko net

Available formats: PDF | BibTeX Citation

Version: 20130402:110947 (All versions of this report)

Discussion forum: Show discussion | Start new discussion
