Towards more aesthetic forms of cryptography

B. Škorić, November 2006

Introduction

When a scientific or engineering discipline reaches a high level of sophistication, it ceases to be a purely function-oriented endeavour and acquires certain aesthetic qualities. Consider for instance robotics. The elegant and efficient motions of sleek robotic arms are delightful to watch. Another example is fractal art. The difference between a sophisticated and an immature discipline is like hearing a song instead of mere speech, reading poetry instead of mere words, seeing a sculpture instead of mere stone.

Cryptography has clearly not yet reached this state of maturity. Not by a long way. Instead of being delightful, it a is messy, painstaking, boring, arduous business for all involved parties, especially for the cryptanalyst. I hypothesize that when cryptography reaches a sufficient state of maturity, reading and analyzing ciphertext will be akin to submerging oneself in a profoundly poetic work of art. Cryptanalysis, even if unsuccessful, will fill the practitioner with joy, while the encrypting and decrypting parties will delight in the beautiful relationships between the plaintext and the ciphertext.

An example

I have tried to construct an example of aesthetically pleasing encryption. The result is of course woefully inadequate, given the current lack of sophisticated tools. One should therefore not judge it per se; I merely intend to point the crypto community in the right direction. The ciphertext below was obtained by applying a humble substitution cipher to a piece of English plaintext. To aid the cryptanalysis, I reveal that the text is about a very popular music gadget that breaks down, and an ensuing conversation.

S fuck ue shit. S dick ly shit.
P'g ejg sg sme'g jlav'x.
Sg jum hvsx u 'poo-poo' asexsex miret;
glue sg jum u arse. S fuck u butty.
“Buddy ly hust, gay nqjsex gfk %&sex gssex”,
must fk, hummsex. S must “lick dick!”. S jum gaysex.
Fk sm weedysex, sme'g fk?
Mi s fuck gfug pdsex-pdsex shit gssex undysex ...
Discussion

Ideally, one would wish to have a cipher (with a short key) that maps natural language as much as possible into artful expressions. Any structure present in the ciphertext should be completely uncorrelated to the structure of the plaintext. The example above fails in these respects.

Having finished the cryptanalysis, the reader will notice that the plaintext, though it is perfectly correct English, sounds somewhat strained and unnatural. Sadly, the awkward wording was necessary to make the example work.

All this reveals how unsatisfying the current state of affairs is. There is a lot of hard work ahead of us!