VETENSKAP OCH KONST

KUNGL
TEKNISKA
HÖGSKOLAN

Numerisk analys och datalogi

March 8, 1996

Anatoly Klepov
Ancort JSC

CERTIFICATE

We have been asked by Ancort JSC to evaluate the data encryption algorithm "LION". We have done so based on a mathematical description of the algorithm as given by a document dated January 7 1996. Aside from this description we have also studied an analysis of the algorithm made by the designer of the algorithm and the key generation procedure.

The main component of the algorithm is a linear feedback shiftregister R_1 which is of length 101 and contains numbers modulo 7. The basic encryption procedure is to generate numbers between 0 and 6 and add them modulo 7 to a representation of the clear text. These numbers are generated 24 at a time and such a set of 24 numbers is called a gamma-vector. A gamma-vector is given by the status of a register R_3 at certain time. The register R_3 is updated through adding certain elements from R_1 and by a polynomial transformation Π and a linear mapping Ψ. It is updated three times before a new gamma-vectors is produced.

The key of the system consists of 101 numbers between 0 and 6 and an initialization vector m. The vector m is sent with the message and is thus not secret. The key is loaded, with the help of a parameter c and m into R_1 at the start of the encryption.

We have analyzed the system and come to the following conclusions.

1. The gamma vectors have desirable statistical characteristics. In particular, the numbers between 0 and 6 appear with equal frequency and there is no correlation between pairs of numbers generated.

2. The mapping from the secret key into R_1 is linear. On the other hand linearity makes it easy to check that some basic properties needed of the system are fulfilled. In particular, that given m all possible R_1 can occur.

3. The heart of the system are the non-linear polynomials Π. They are applied twice to key dependent inputs before the first encryption is performed. It is our estimate that, given a suitable choice of Π, Ψ and c, this introduces sufficient nonlinearity into the system to prevent an attacker from exploiting the linearity of loading the key into R_1. In such a case we see no possible way to break the system using a feasible time of computation, say less than the age of the universe on a modern high-speed computer.

Stockholm, March 8, 1996

Johan Håstad

Johan Håstad
Professor of Theoretical Computer Science.
Specialty:Efficiency of computation and
cryptography

VETENSKAP OCH KONST