ABSTRACT

SARI AGUSTINI HAFMAN. The Uses of Markov Chain in the Development of Key Predictability Test Methodology. Supervisors: ANANG KURNIA and AGUS BUONO.

One Time Key (OTK) system with key from alphabetical sequences is one of symmetric encryption algorithm that used in Indonesia to protect secret information until now. Alphabetic sequences in OTK system must be cryptographically secure pseudorandom sequences. OTK system in Indonesia only tested by overlapping m-tuple test developed by Marsaglia (2005). Overlapping m-tuple test doesn’t check the unpredictability of alphabetical sequences, it just tests distribution form and independency of alphabetical sequences. So, alphabetical sequences in OTK system cannot be used in cryptography application by the reason of unpredictability sequence is unknown. Because some of Pseudorandom Number Generator (PRNG) algorithm based on block cipher algorithm that has markovian properties, markov chain model used to detect predictability alphabetical sequences.

Data in this study consists of two data sources i.e. simulation data that generated from four classes PRNG and OTK system keys in 2005 that used in three communication units of foreign ministry. Simulation data is used to develop key predictability test methodology by find predictability threshold value based on characteristic of match level. OTK system keys will be predictability tested by comparing characteristic of match level with threshold value that is obtained from simulation data.

The first result of this study shows the alphabetical sequence generated by first, second and fourth PRNG class can’t be modeled with first-order markov chain until third-order. The third PRNG class, except PRNG LCG1, LCG2, coveyou, rand and randu, also can’t be modeled with first order markov chain until third-order. Sequence generated by LCG2, coveyou, rand and randu are not fit for use in cryptography because it has a high probability to be modeled by high orders of markov chain (above the order of three). The second result obtains predictability threshold value with markov chains based on the minimum and maximum match level on the second-order and third-order. The last result shows the size of training data must be greater than the size of the observation data with the best ratio between the size of training data with observational data is 100: 10.

The results of testing using 10 times repeated shows that the match level average of the OTK system key match on the all of three-order less than 4.5 x 10^{-2}, so the OTK system the is feasible to secure information in three communication units.

Keywords: One Time Key (OTK), markov chain, PRNG, probability transition, match level