Topic: Cryptography

Preferred presentation mode: Oral

**Statistical Correlation Analysis of Encryption Strength and Key Size in Modern Cryptosystems**

*Md. Jubairul Alam1\* and Md. Mortuza Ahmmed2*

*1Department of Computer Science, American International University-Bangladesh, Dhaka, Bangladesh*

*2Department of Mathematics, American International University-Bangladesh, Dhaka, Bangladesh*

*\*Email: 22-48238-2@student.aiub.edu*

**Abstract**

**Objective:**

The aim of this research is to examine the relation of the encryption strength and the key length in today’s cryptosystems with special emphasis on the popular algorithms which are RSA, AES and ECC. The goals of the study are to assess the degree of increase in maximum key length and the effects it has on the strength architecture against cryptographic attacks, computational efficiency, and security through envisaging the findings by means of statistical correlation analysis.

**Methods:**

A dataset that consists of Performance parameters of encryption algorithms in terms of key size and encryption strength is obtained from the efficiency and attack simulation results. In order to determine and quantify dependence of brute force and algorithm specific resistance on the key length, Pearson and Spearman correlation coefficients among other statistical correlation techniques are utilized. In order to quantify key strength, regression models are employed in terms of each scenario (e.g., under low-resource environments vs. explosive encryption strength requirements.

**Results:**

The first evaluation indicates that there is a broad positive relation between key size and strength of encryption for all the crypto systems analyzed, although there are some trends of decreasing return as key sizes become very large. The research highlights key size range that is appropriate in terms of saving resources used with added security. More importantly, ECC is observed to be more efficient in key size usage relative to strength than RSA and AES.

**Conclusion:**

This statistical analysis sheds some light on the significance of a key size in fulfilling the requirements of an encryption algorithm. The results highlight the need for selection of appropriate key sizes with regard to use-cases, and provide useful recommendations for developers and security practitioners aimed at achieving optimal cryptographic implementations. The research also aims at furthering the knowledge of the design of cryptosystems by trying to make a quantifiable relation between key size and encryption processes.

**Keywords:** Cryptosystem efficacy, Statistical correlation, Key size optimization, Encryption strength, Predictive modeling.