ELUCIDATION OF THE INFEASIBILITY OF QUANTUM CRYPTOGRAPHY CRACKING RSA-2048

Abstract

RSA is the most widely used encryption algorithm up to date, being upgraded, has kept its reputation by being unbreakable for a long time, but the new coming of quantum cryptography is believed, & publicly stated to be the one to break it.

It’s said that in the near future Quantum Computers will have ability to, debug immersive lines of code, instantly break an amount of encryption, break any type of encryption etc. But, until now, other than some theoretically predicted proving’s, there’s no legitimate practical proof to express that classical cryptographic methods have been broken.

Introduction

RSA, or **Rivest-Shamir-Adleman Algorithem** is a cryptographic algorithm used, since the 1970s, for the benefit of protecting sensitive data, from being exposed. RSA preserves the CIA triangle in communication & protecting of data. This algorithm takes in to consideration, both the symmetric & asymmetric features in usage, by using asymmetric key for encryption & symmetric for the opposite. Even though the techniques use, might slower the transaction within, this method holds the reputation of unbreak-ability & hence renowned as an extensively used algorithm in data protection.

Quantum cryptography focusses more on the probability, rather than checking the binary values 1/ 0. It’s faster, & processes more data, in comparison to the genuine computers nowadays. A Qubit, is produced via operating upon a quantum state of an object, which basically is an undefined property of an object that’s been perceived. For clarity, something like the photon, divergence. Other objects can be entwined to these superpositions. The un settled states can be later, translated to a complex sector of mathematics, which can later be glued together with special algorithms, for solving problems.

Research Problem

This study here will focus on the RSA algorithms, and quantum cryptography, understanding its capacities, capabilities, misbeliefs & in the end, expectantly prove that, though quantum cryptography seems like the best encryption/ decryption method, there’s no chance, that quantum cryptography could break RSA at the moment.

Objectives

Even though, Quantum Cryptography seems to be breaking down all boundaries, the main focus behind this literature is to prove, that quantum cryptography will not be feasible to crack open RSA.

Methodology

1st of all, ill be talking about how RSA works, then to proceed to see how QC works. Ill talk about the facts & Figures of the myths, I’ll talk about the infeasibilities to proceed with how things actually work. To conclude, ill discuss whether the topic is indeed correct, & that there’s no present risk to RSA been broken.

Suitable References

[1] RSA (cryptosystem). (2020, April 20). Retrieved from <https://en.wikipedia.org/wiki/RSA_(cryptosystem)>

[2] M. Korolov and DougDrinkwater, “What is quantum cryptography? It's no silver bullet, but could improve security,” *CSO Online*, 12-Mar-2019. [Online]. Available: https://www.csoonline.com/article/3235970/what-is-quantum-cryptography-it-s-no-silver-bullet-but-could-improve-security.html. [Accessed: 22-Apr-2020].