Tu-vera: An Encryption Algorithm Using Propositional Logic Calculus

Maria Vargas-Vera, Independent Researcher, Milton Keynes, UK

ABSTRACT

This article describes how the encryption algorithm (called Tu-vera) depends on the transformation of a phrase written in English into a sequence of propositional logic formulas which can be understood by a human receiver. This happens if the receiver has a set of reserved words and he/she knows the level of unfolding manipulation that the receiver needs to perform in the transformation of the phrase/sentence. The Tu-vera algorithm requires several steps like a) to give a phrase; b) to re-order words of the given phrase in order to form a propositional logic formula; c) to make use of background knowledge by performing substitutions; d) to answer questions in general subjects (like literature, biology and so forth); e) to change synonyms/antonyms (if this is feasible); f) to perform actions in order to give value to both or one operand of the logic formula and g) to conclude the final answer of the logic formula (true or false) depending of the logic values of the operands in the logic formula. Finally, a working example, in the subject of universal history is introduced.

KEYWORDS

Caesar Cypher, Cryptography, Encryption Algorithms, Information Extraction, Propositional Logic Calculus, Tukhachevsky Encryption Algorithm, Vigenere Cypher

INTRODUCTION

The importance of exchange data over the internet and other media is motivating the search for efficient solutions to offer security and protection against data thieves’ attacks. The algorithms used to protect data/information are called (in the literature), encryption algorithms. Encryption algorithms have become popular between companies /organizations as a means of keeping confidential information safe. The literature offers a variety of encryption algorithms such as, Blowfish, AES, RC4, RC5, RC6 and so forth. By the use of an encryption algorithm, the information is made into meaningless cypher text and requires the use of a key to transform the data back into its original form. According to Wiesmaier (Wiesmaier, 2001), the level of security offered by an encryption algorithm is not proven mathematically instead the assessment is based on robustness against known attacks. The more an algorithm is tested the most trustworthy it is considered. However, the security of a given cypher text depends greatly of the secrecy of the decryption key. In general, longer keys offer better security (against brute force attacks) but, usually decrease the performance. The encryption algorithms are

DOI: 10.4018/IJSEUS.2018040105

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
classified in symmetrical and asymmetrical. The symmetric algorithms use the same key for encryption and decryption and usually have predefined key lengths. Symmetric algorithms provide high security and performance but these algorithms have the problem that they require the exchange of a key.

We present a novel encryption algorithm named “Tu-vera” which makes use of the first order logic calculus. The main idea of our proposed encryption algorithm is to transform a sentence/phrase written in English into a first order logic formula. In order to clarify, our algorithm, we have defined a working example by defining several phrases in the subject of universal history and theme the First World War (WWI). The working example covers the theme of WWI, but, our Tu-vera algorithm (version 2) could be used to encrypt a full document which can be sent to a receiver who could decrypt the message and get back to the original information. The main contribution of the Tu-vera algorithm (version 2) is that, it does not require a “key” for encryption. Then, our proposed Tu-vera algorithm (version 2) has the promise to go beyond the current encryption algorithms. The paper is organized as follows: Firstly, we describe related work. This section shows related work from two streams, from the viewpoint of encryption algorithms and related work in propositional logic calculus. Secondly, we present a working example using our proposed algorithm. The working example uses universal history and the theme is WWI. Thirdly, we present our novel algorithm called “Tu-vera” (version 2). Fourthly, we present a discussion about how our algorithm can be used in information extraction patterns. Fifthly, we show a preliminary evaluation and finally, we state our conclusions and future work.

RELATED WORK

The section of related work is organised in two streams namely, a section of first order logic calculus and a section of encryption algorithms.

Mathematical Logic

**Definition 1:** A Model is a set $D$ and a function $f$ such that:

- The function $f$ assigns each constant to a member of $D$.
- The function $f$ assigns each unary predicate to a subset of $D$.
- The function $f$ assigns each binary predicate to a subset $D \times D$.

The basic idea is that a set of constants and predicates are paired with elements from the set of elements of the model. In other words, each constant can be paired directly with an element of the model. For example, if our model includes an individual called John, then, we might pair the constant “$a$” with the individual John.

Let us consider predicates. An expression like $G(a)$ is true just in case $f(a)$ is in the subset of $D$ that $f$ assigns $G$ to. For example, if “$a$” is paired with “John” and John is in the set of $D$ that $G$ is paired with, $f(a) = John$ and $John \in f(G)$, then $G(a)$ is true.

In the same way, $H(a, b)$ is true just in case “$(a, b)$” is in the subset of $D \times D$ that $f$ assigns $H$ to. For example, if we take $D$ to be the set of words of English and we take $H$ to be the relation has fewer letters than, then $H(a, b)$ is true just in case the elements we pair constant “$a$” and constant “$b$” which are in the set of ordered pairs defined by $f(H)$. For example, if $f(a) = table$ and $f(b) = vase$, then $(table, vase) \in f(H)$ and $H(a, b)$ is true.

Note that there is not requirement that there be a single model. AQ logical system can be paired with any number of models. A more detailed description can be found in (Mendelson, 2009).

Cryptography

Cryptography is associated with scrambling plaintext into a cipher text (a process called encryption). Cryptography enables sharing confidential information between entities in open networks such like
Boundary Critique and Stakeholder Collaboration in Open Source Software Migration: A Case Study
Osden Jokonya and Stan Hardman (2013). Knowledge and Technological Development Effects on Organizational and Social Structures (pp. 194-208).
www.igi-global.com/chapter/boundary-critique-stakeholder-collaboration-open/70570?camid=4v1a

Patient Experiences of Diabetes eHealth
www.igi-global.com/article/patient-experiences-of-diabetes-ehealth/112016?camid=4v1a

GIS and GPS Applications in Emerging Economies: Observation and Analysis of a Chinese Logistics Firm
www.igi-global.com/article/gis-gps-applications-emerging-economies/45876?camid=4v1a