**Reducing risks of data theft : Hashing vs. Asymmetric encryption**

**Research Methods**

Student Name : Sagarika Nagaraj

Student ID : 17061633

**Abstract**

**Comment :** The first two sentences are far too general and very hard to understand. You need to be much more concrete and name the problem you are trying to solve - rather than vaguely hinting at it. It is hardly possible to tell that this is about cryptography.

**Response** : I replaced the two sentences with the below two lines. The concept is more clear now because here I have mentioned about the stealing of the data. Personal and confidential information stealing is a crime.

( Data theft is basically an act of stealing data that is stored on computers or other devices from an unknowing victim with the aim to hack personal or confidential information. )

**Comment :** What is “aligned infrastructure”? Never heard this expression before. Infrastructure aligned with what?

**Response :** This was wrong sentence. I removed it.

**Comment :** Later you say “these alignments”, but which alignments do you refer to? The alignment between infrastructure (which precise infrastructure are you talking about?) and “mechanisms of hashing”?

**Response :** I was unable to explain it with the wording before. Actually aligned infrastructure basically consists of the details of architecture, reliability and security. The alignment requires skills in delivery and support areas as well as in the areas of flexibility and agility.

(This measure of protection is the consideration which is developed on the bases of aligned infrastructure and the mechanisms of hashing and asymmetric course of interactions are to be weighed. Aligned infrastructure is basically consists of the details of architecture, reliability and security)

**Comment :** “in direction for the keys”? What does that mean?

**Response :** In this paper, we will look at different methodologies for the protection of data. The Password-Based Key Derivation Functions (PBKDF) is carried out in this study of the functions through which the passwords are transmitted into secret keys. This process tends to maintain the fixed size cipher function of operation. Other queries of the abstract are also solved in this part.

**Introduction**

**Comment :** I (and presumably Felix too) don’t understand what you mean when you say “programs ... depict .. bases of encrypted security of the user information”? What precisely are these programs depicting? The basis of any encryption algorithm is not an easily visualisable thing. What you - or a program - can show is a hash sum, some hexadecimal key or the like.

**Response :** This all is replaced with the new wordings now it will be more clear to you. Digital security could be working out of ensuring PCs, workers, cell gadgets, electronic frameworks, sites, and information from noxious attacks. It is likewise called security or data assurance that is electronic. Encryption might be the manner by which data is changed into key code that conceals the subtleties' genuine importance. The innovation of encoding and data that is decoding called cryptography. In processing, decoded data can be called plaintext, and scrambled data is named cipher text.

**Comment :** Next sentence: “protected with the course of evaluation”: again, this is an expression that I really don’t understand. You can evaluate a cryptographic algorithm as to whether it really works (or whether is has security holes), and there are methods, typically cryptographic ones, to protect a password. However, you cannot protect passwords through evaluation - the process of protecting a password in some manner, and he process of evaluating the protection process are two categorically different things

**Response :** Yes these two the different things. We will use cryptographic solutions to solve this issue now I have written in a clear way.

**Comment :** “In the same manner ..”: Again, I don’t understand this sentence, and when trying to understand why I don’t understand it it is for two reasons: 1. some expressions such as “procedures of different bases” are overly general and therefore close to meaningless. However, this expression is not just very general sounding, but also: we normally don’t speak of “procedures of bases”, maybe because both ‘procedure’ and ‘basis’ are in themselves already quite general. Usually the are combined with other, more concrete words such as “closing procedure” or “opening procedure” of a campus for example, or “the basis of modern mathematics”, “the basic ingredients of a cake”, “the basis of modern democracy”, etc. There are more sentences that I don’t understand but I can’t analyses every single one of them as this would take me too much time.

**Response :** I have changed all the intro part please have a look.

(Hashing is certainly a calculation done on information like a message or record to deliver a volume called a hash (alluded to as a checksum). The hash is utilized to check that information isn't adjusted, messed with, or ruined. Spot another genuine way, you will approve the information has looked after uprightness) its more clear now.

**Research Question**

**Comment :** I’m not a specialist in cryptography, but hashing is used also outside of cryptography. However, I would have thought that, if hashing still plays a big role in cryptography, its advantages and disadvantages would have been explored since a while. Is this really an open question? And, I think, you wanted to say “application” rather than “implication” here.

**Response :** Yes there are advantages and disadvantages too. But when we use hashing for the data security purpose, it will be more beneficial for security.

(Can the data be protected by implementing the applications of hashing and asymmetric encryption? )

**Comment :** Typically you state aims and objectives first, before the research question, if you want to state these at all (you don’t need to)

**Response :** I swap them now. Its logical now.

**Comment :** “The assessment of the ...”: This is very, very general. I assume there are dozens of different methods and approaches to protect data from being stolen. Given the generality of this objective, you would need to analyze every single one of them, which would be a major endeavor if I am correct in that there are many such methods. So this would most certainly be too much for a MSc thesis.

**Response :** There are number of practices by using which we can protect our data from stealing. In this paper, we are focusing on the applications of hashing and asymmetric encryption. This research will highlight the following aims and objectives:

The evaluation of different securing measures for data from theft.

Analyzing the security of data through hashing.

Assessment of security of data through asymmetrical encryption.

**Background**

**Comment :** “The build of background”: this is “meta-talk” again (see above). Don’t topicalize the general way in which you write or wrote the background IN the background section. Best, delete this sentence

**Response :** I have deleted the sentence.

**Comment :** I also don’t understand the rest of this paragraph. How did you write this? Was there some automatic translation involved?

**Response :** no sir there is no auto translation involved. It is just a bad English. I improved it now please have look.

**Comment :** Paragraph 2 : I was not aware that ATM password hacking was a big thing - at least it doesn’t seem to be in the UK or the rest of Europe as far as I’m aware. However, I might be wrong. This is why you should add a citation here, otherwise people may not believe you.

**Response :** Citation is added now.

**Literature Review**

**Comment :** You don’t need this section as you are not doing a structured literature review. Incorporate this section in the background.

**Response :** This section is merged in the background part.

**Methodology**

**Comment :** Research Approach: What is ‘subjective analysis’ or ‘subjective methodology’? Never heard of this before. I double-checked in the book you cite (Leavy) but I can’t find this method there neither 1. par: “Remaining ..” This sentence is nonsensical: delete ore rewrite You mention ‘subjective research’ again: I don’t know that this is ought to be, but I would have thought that quantitative methods to evaluate cryptographic algorithms would be more established in cryptography.

**Response :** This all is replaced according to the requirements.

Hashing is one of the complex topics in the field. The methodology which is used to create this paper was the qualitative methodology. Qualitative methodology is one of the most advance tool and technique that helps incomplete research. It is important to understand that there is a proper need for a brief analysis about which the content has been already published and these studies are analyzed to prepare this study. There are four types of qualitative methodology which uses in the paper. Methodology is a necessary part that helps in identifying the problems regarding the technology.

One of the main reason to write this paper is to identify the issue which is involved in the problem. There are four types of techniques that have been used in qualitative technology. It is important to understand these all four types of tools helped to complete this research. The most common type of qualitative research is phenomenology. This type of research involves in development of the brief theory. Furthermore, it can be said the qualitative methodology is one of the helpful tools for the development of the research.