Principles of Cryptography

Students Name

University

Course

Professor

Date

Principles of Cryptography

Even 2000 years ago, encryption already existed. A famous example is Caesar's shift cipher (Delfs and Knebl, 2006). Every transaction runs with both algorithms of encryption (A) and decryption (B) as well as a secret key (m). This method is called symmetric encryption. The mathematical equation for Caesar's cipher is given by:

$$B(m,\mathrm{A}(m,n)) = n \text{ for each plaintext } n.$$

The main objective of cryptography is not just data privacy and security; it also includes integrity, authentication, and non-repudiation (Delfs and Knebl, 2006). Cryptanalysis is the study of various attacks used to counteract cryptography, and it can be easily seen as cryptology, the principle governing cryptology first stated by A. Kerckhoffs (Delfs and Knebl, 2006). Kerckhoffs's principle explains that though cryptography allows the secrecy of pieces of information, there is someone who will hack the system. The provable vulnerability of security was attested by the information theory designed by C.E. Shannon.

Cryptography uses a probabilistic or deterministic algorithm. The probabilistic algorithm is used by hackers, and to counterfeit it, the deterministic algorithm is implemented. The deterministic algorithm D is acquired by x and y and uses the mathematical mapping:

$$D : x \rightarrow y$$

The output y is computed through the input x as a finite number. Delving deeper into the probabilistic algorithm, it is composed of three real-life probability schemes, namely, the Coin-Tossing algorithm, the Monte Carlo, and Las Vegas algorithm. The Coin-Tossing algorithm is biased because it can only supply two choices, and to explain further, the mathematical mapping for coin-tossing is defined as:

$$\mathrm{prob}(D(x) = y) := \mathrm{prob}(\{\mathrm{r} \mid \mathrm{D_A}(x, \mathrm{r}) = y\}).^2$$

The probabilistic algorithm *D* depends on the output *y* concerning the input *x* and the string binary *r*. For a random event, "*D* outputs *y* on input *x*", which raises a question of what is meant. Whereas with the Monte Carlo and Las Vegas algorithms, any event P with the probability of probabilistic algorithm *D* as an input of *x* is equal to the summation of the coinciding probabilistic algorithm *D* to its input *x* is the same as the output *y*.

$$prob(D(x) is\ a\ correct\ answer\ to\ P = \sum_{y \in y_x} prob(D(x) = (y)$$

Information Theory plays a vital role in the consideration of how data will interfere in the algorithm system. The probability inclusion of *X* simply states that in a random experiment, the possible outcome we can gain in the proposition is jointly distributed.

$$H(X) = \sum_{x \in X,\, prob(x) \neq 0} prob(x) * log_2\left(\frac{1}{prob(x)}\right)$$

The permutation algorithm is the simplest example of how encryption works. The alphabetical letters are considered to be the basis for deciphering plaintext messages. This is how the word BOB can be extracted into the permutation cipher.

a b c d e f g h I j k l m

b c d f g h j k l n o p r

n o p q r s t u v w x y z

s t v w x a e i z m q y u

To understand more about cryptography, see the abstract algebra example below on how exactly to decode a cipher. Translate EAT AT JOE'S. Note the focus on the digraphs (length = 2, vector = 2).

$$A = [5\ 1\ 8\ 7\ ],\ B = (5, 3)$$

This is then translated into,

4, 0, 19, 0, 19, 9, 14, 4, 18.

And the units are:

(4,0), (19,0), (19,9), (14,4), (18,18).

The determinant of matrix A is 1, by applying the map *f(v) = Av + B;*

$$A\begin{pmatrix}4\\0\end{pmatrix} + B = \begin{pmatrix}5 & 1\\8 & 7\end{pmatrix}\begin{pmatrix}4\\0\end{pmatrix} + \begin{pmatrix}5\\3\end{pmatrix} = \begin{pmatrix}20\\32\end{pmatrix} + \begin{pmatrix}5\\3\end{pmatrix} = \begin{pmatrix}25\\9\end{pmatrix}$$

The message we now get is:

(25,9), (22,25), (5,10), (1,13), (9,13).

Now, convert it to digraph:

(Z,J), (W,Z), (F,K), (B,N), (J,N).

Encrypting it gives you,

EAT AT JOE'S → ZJWZFKBNJN

References

Delfs, H., & Knebl, H. (2015). *Introduction to Cryptography Principles and Applications*. Springer Berlin Heidelberg.