CS575: Final Project Report

Project Title: Blowfish Algorithm and DSatur Algorithm

Team Member(s): Rahul Verma

I. Problem

1. Blowfish is an encryption technique designed by Bruce Schneier in 1993 as an alternative to DES Encryption Technique. It is significantly faster than DES and provides a good encryption rate with no effective cryptanalysis technique found to date. It is one of the first, secure block cyphers not subject to any patents and hence freely available for anyone to use. Blowfish Algorithm is used for Bulk Encryption, Packet Encryption(ATM Packets) and Password Hashing. Blowfish is a fast block cipher except when changing keys. Each new key requires a pre-processing equivalent to 4KB of text, it is faster and much better than DES Encryption [3]."

2. DSatur is a graph coloring algorithm put forward by Daniel Brélaz in 1979. Similarly, to the greedy coloring algorithm, DSatur colors the vertices of a graph one after another, adding a previously unused color when needed. Once a new vertex has been colored, the algorithm determines which of the remaining uncolored vertices has the highest number of colors in its neighborhood and colors this vertex next. Brélaz defines this number as the degree of saturation of a given vertex. The contraction of the term "degree of saturation" forms the name of the algorithm. DSatur is a heuristic graph coloring algorithm, yet produces exact results for bipartite, cycle, and wheel graphs [7].

II. Algorithms

1. Steps involved in Blowfish Algorithm are as follows:

a) Initially, the input consists of x number of characters and space if present.

b) The input is split into 32 bits. The left 32 bits are XORed with P1, which is generated by key expansion to create a value called P1.

c) P1 runs through a transformative F-function (F In) in which the 32 bits are split into 4 bytes each and passed to the four S-boxes.

d) The first two values from the first two S-boxes are added to each other and XORed with the third value from the third S-box.

e) This result is added to the output of the fourth S-box to produce 32 bits as output.

f) The output of F In is XORed with the right 32 bits of the input message to produce output F1'.

g) F1' replaces the left half of the message, while P1' replaces the right half.

h) This same process is repeated for successive members of P-array for 16 rounds in total.

i) After 16 rounds, the outputs P16' and F16' are XORed with the last two entries of the P-array, i.e., P17 and P18. They are then recombined to produce the 64-bit ciphertext of the input message [4].

2. Let the "degree of saturation" of a vertex be the number of different colors being used by its neighbors. Given a simple, undirected graph G compromising a vertex set V and edge set E, the algorithm assigns colors to all of the vertices using color labels a, b, c and so on. The algorithm operates as follows:

Step 1: Let v be the uncolored vertex in G with the highest degree of saturation. In cases of ties, choose the vertex among these with the largest degree in the subgraph induced by the uncolored vertices. Assign v to the lowest color label not being used by any of its neighbors. If all vertices have been colored, then end; otherwise return to Step 1.

Step 2: of this algorithm assigns colors to vertices using the same scheme as the greedy coloring algorithm. The main differences between the two approaches arises in Step 1 above, where vertices seen to be the most "constrained" are colored first [7].

III. Software Design and Implementation

A. Software Design

1. Blowfish Algorithm Design is as follows:

A 64-bit plaintext message is first divided into 32 bits. The "left" 32 bits are XORed with the first element of a P-array to create a value P', run through a transformation function called F, then XORed with the "right" 32 bits of the message to produce a new value F'. F' then replaces the "left" half of the message and P' replaces the "right" half, and the process is repeated 15 more times with successive members of the P-array. The resulting P' and F' are then XORed with the last two entries in the P-array, and recombined to produce the 64-bit ciphertext [5].

2. The DSatur Algorithm Design is as follows:

Let v be the uncolored vertex in G with the largest saturation degree. In cases of ties, choose the vertex among these with the largest degree in the subgraph induced by the uncolored vertices. Further ties can be broken arbitrarily.

Assign v to color i, where i is the smallest integer from the set that is not currently assigned to any neighbor of v.

If there remain uncolored vertices, repeat all steps again, otherwise, end at this step [9].

B. Implementation and Tools Used

1. Implementation of Blowfish Algorithm consisted of 2 major components: Encryption and Decryption

a) Encryption was implemented in this particular order:

Step 1: Generation of Subkeys

Step 2: Initialize Substitution Boxes

Step 3: Encryption

The encryption function consists of two parts: Rounds and Postprocessing

b) Decryption was implemented in this particular order:

Decryption works in reverse as compared to Encryption in Blowfish Algorithm.

Step 1: Generation of Subkeys

Step 2: Initialize Substitution Boxes

Step 3: Decryption [3]

2. The implementation of DSatur Algorithm consisted of a choose function which chooses one of the available colors for the vertex, addedges function which adds edges between two vertices and takes 2 parameters a and b, function for creation of vertices and dsaturalgorithm function which computes various things like availability of colors, vertex chosen, degree of saturation incrementation. Used Visual Studio Code for both the algorithms.

C. Performance Evaluation (Optional)

IV. PROJECT OUTCOMES

- https://youtu.be/UENuEqX_HEE
- https://docs.google.com/presentation/d/1aBTwmwpU2wVvMaXFdlhJh49SiJuleXNe/edit?usp=sharing&ouid=116627601689585637909&rtpof=true&sd=true

REFERENCES

[1] Schneier, B. (1994). Description of a new variable-length key, 64-bit block cipher (Blowfish). In: Anderson, R. (eds) Fast Software Encryption. FSE 1993.

[2] https://en.wikipedia.org/wiki/Blowfish_(cipher) (reference pseudocode)

[3] https://www.geeksforgeeks.org/blowfish-algorithm-with-examples/ (reference code)

[4] https://www.techtarget.com/searchsecurity/definition/Blowfish

[5] https://www.design-reuse.com/articles/5922/encrypting-data-with-the-blowfish-algorithm.html

[6] Brélaz, Daniel. “New methods to color the vertices of a graph.” Commun. ACM 22 (1979): 251-256.

[7] https://en.wikipedia.org/wiki/DSatur (reference pseudocode)

[8] https://www.codingninjas.com/codestudio/library/dsatur-algorithm-for-graph-coloring (reference code)

[9] https://www.geeksforgeeks.org/dsatur-algorithm-for-graph-coloring/ (reference code)