Performance Analysis of Mail Clients with RSA and ElGamal using SNORT

K. Sreerama Murthy
Research Scholar, CSSE, AU, Visakhapatnam

S. Pallam Setty, PhD
Professor CSSE, AU, Visakhapatnam

G. S. V. P. Raju, PhD
Professor, AU, Visakhapatnam

ABSTRACT
Internet is one of the boons to society and companies to move into an age of reliable and open communications. This open communication sometimes produces vulnerabilities and glitches such as financial losses, reputation damage, service availability maintenance, guarding the customer data and personal data and much more, and rushing both organizations and service providers to take necessary steps to protect their important data from intruders, hackers, and insiders. Intrusion Detection System has become the mandatory need for the successful content networking. SNORT is one of the open source tool for detecting malicious activities. It prevents users or source IP addresses from entering into the network. This project applied encryption for text files by using cryptographic algorithms like ElGamal and RSA. It has been observed that Snort is effective for compressed data for both the algorithms. It has been found that as the size of the file increases, the run time is constant for compressed data, whereas in plain text, it varied drastically.

General Terms
Intrusion Detection System, encryption algorithms

Keywords
IDS, IPS, SNORT, Mail

1. INTRODUCTION
1.1 Intrusion Detection System
An Intrusion Detection System (IDS) is a software scheme or application that observes system or network events for malignant actions or policy desecrations and gives reports to a management station. Intrusion detection and prevention systems (IDPS) are majorly concentrated on finding probable incidents, recording the data about the incidents, and reports the attempts. Free Intrusion Detection Systems:

Free Intrusion Detection Systems:

- ACARM
- AIDE
- Bro NIDS
- OSSEC HIDS
- Prelude Hybrid DS
- Samhain
- Snort
- Suricata

NIDS:
NIDS is meant for identifying malicious activities within the network and it observes the packet flow over the network, which are usually overlooked by a firewall.

HIDS:

HIDS observes the activities on individual machine where the IDS got fixed. It verifies activities like login attempts, machine call trace, schedules of processes etc., Two types of IDS are grouped together to form a Hybrid IDS.

SNORT is a freeware network intrusion detection system capable of performing real-time traffic investigation and packet recording on IP networks.

2. PROBLEM STATEMENT
Packet analysis can be done by Snort. In Snort, concentration has been on sniffer mode in this project. In Sniffer mode, Snort will read the network information and shows on console. Snort is the best Network Intrusion Detection System with other systems. In this project, the performance of different mail clients has been measured by using Snort. In the simulation study, the project considered three mail clients (Gmail, Yahoo, Hotmail). By varying the text sizes from 50 kb to 2mb for all the three mail clients, it has been found that runtime is less when the mail client Hotmail is used.

Again SNORT is applied by using cryptographic algorithms to encrypt plain text using ElGamal technique and RSA. From simulation results, it is observed that for compression data the impact of SNORT is very less.

3. SNORT OVERVIEW
3.1 SNORT
Snort is a freeware signature based Network Intrusion Detection System(NIDS), created by Martin Roesch in 1998. Snort performs actual data packet investigation and packet recording on IP networks. Snort performs protocol investigation, content verification, and content match and notices different kinds of interventions and reviews like stealth port scans, buffer overflows. Snort can be configured in three main modes: sniffer, packet logger, and network intrusion detection.

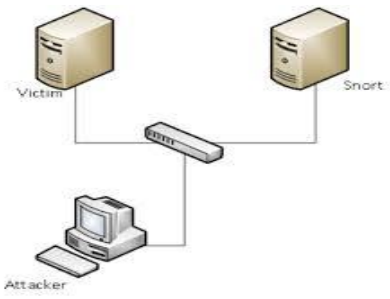

Fig 1: SNORT structure

3.2 SNORT Modes

SNORT runs in different modes like:

3.2.1 Sniffer mode

It reads the packets from the network and displays them on the console.

Options:

$ sudo snort –v

Prints TCP/IP header on to console (also for UDP /ICMP).

$sudo snort –vd

Prints the application data as well.

$ Sudo ./snort –vde

Prints the data link layer contents as well.

3.2.2 Packet Logger mode

Packet logger mode records the packets to the disk.

Options:

$ sudo snort –dev –l ./log

Logs the packets to the directory specified.

$ Sudo ./snort –l ./log –b

Binary log, binary file may be read back using –r switch

3.2.3 IDS mode

Snort provides near real-time intrusion detection capability with IDS mode.

Options:

snort -c /usr/local/share/snort_rules/rules/snort.conf

4. MAIL CLIENTS

An email client, email reader, or more formally Mail User Agent (MUA), is a computer program used to access and manage a user's email.

In addition, a web application that provides message management, composition, and reception functions is sometimes also considered an email client, but more commonly referred to as webmail.

Popular web-based email clients: Gmail, Yahoo! Mail, mail.com, Lycos mail, and Hotmail

4.1 Gmail

Google has provided a free, advertising-supported email service called Gmail. Gmail can be accessed as a secure webmail via POP3 or IMAP4 protocols.

4.2 Yahoo

Yahoo! Inc. is an American MNC company and its business is mainly into website portals, search engines.

Products and services:

- Storing personal information and tracking usage
- Communication
- Content
- Mobile services
- Content
- Advertising

4.3 Hotmail

Outlook.com (previously MSN Hotmail, Windows Live Hotmail and Hotmail) is a freeware email facility running by Microsoft corporation. It was renamed to "MSN Hotmail". Outlook.com is the new name given to HotMail after merging of Windows Live suite.

5. ENCRYPTION

While data is traveling among multiple systems, the safety of data is of high priority. While the data is traveling before reaching the destination, attackers could modify or forge the data.

- **System Safety**- Combination of tools for protecting information.
- **Web Safety**- Safeguards information while communication.
- **Internet Safety** – Safeguards information while communicating through a pooling of network Security issues.
- **Safety assault** – An event which concise the safety of Data.

There are two basic varieties of encoding patterns: private-key and asymmetric-key encoding. The encoding and decoding keys are similar in private-key schemes patterns. Thus both sender and receiver synchronize upon a cryptic key whenever they want communication. In asymmetric-key patterns, the encoding key is disclosed to encode data whereas the consumer has the decryption key and can read encoded data. Asymmetric-key encoding is a new innovation: all encoding patterns are asymmetric-key/symmetric key patterns.

5.1 ElGamal

An asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange is the ElGamal encryption system. ElGamal encryption consists of three components: the key generator, the encryption algorithm, and the decryption algorithm.

Efficiency:

ElGamal encryption is probabilistic encryption i.e. a single plain text can be encrypted to many possible cipher texts and that a general ElGamal encryption methodology produces a 2:1 expansion in size from plain text to cipher text. ElGamal's encryption has two exponentiations where these exponentiations are independent of the message and can be computed ahead of time if required. The Decryption requires only one exponentiation.

5.2 RSA

RSA is an algorithm for public-key encoding scheme built on factoring large integers problem. RSA is based on product of 2 large prime numbers, along with a helping value as public key.

Need to maintain secrecy for the selected two prime numbers. The RSA algorithm involves three steps:

- Key generation, encryption and decryption.

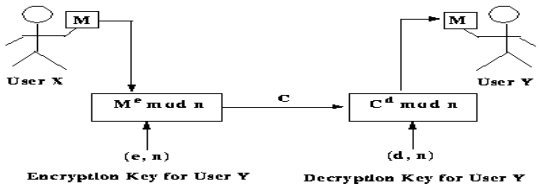

Fig 2: Encryption process

6. EXPERIMENTAL RESULTS

6.1 SNORT with ElGamal Technique

In this project, an experiment been carried out to analyze the data from SNORT by sending plain text and encrypted files separately of different sizes (50kb, 100kb, 500kb, 1mb, 2mb) in Gmail, Yahoo and Hotmail mail clients.

Firstly, the text files are sent and the data produced by SNORT is compared to the data of encrypted files.

Applying ElGamal Technique in Gmail with SNORT

Following is the table of analysis of data produced by SNORT when files are sent through Gmail. The first row is the data of plain text sent. The second row is the data of corresponding encrypted text using ElGamal

Total packets-ElGamal-Gmail

Total packets are the total number of packets received by the SNORT from the network.

Table 1: Total packets ElGamal-Gmail

Size	50kb	100kb	500kb	1mb	2mb
Plain text	225	295	776	1866	2612
Encrypted	119	113	114	222	252

GRAPH:

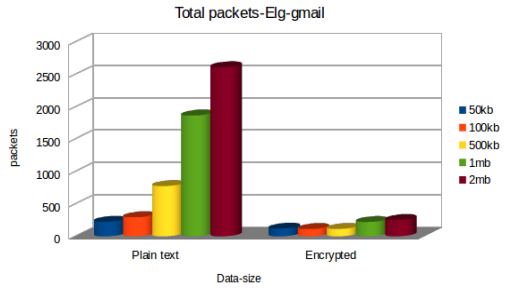

Fig 3: Total packets ElGamal-Gmail

In the above graph, the total packets received by SNORT is higher for plain text when compared to encrypted text which increases the runtime, and memory is also occupied more in that case.

Analyzed Packets:

Analyzed packets are the packets analyzed by SNORT during runtime. SNORT does not analyze all the packets received by the Ethernet; it drops some of the packets that are needed to be buffered for processing.

Following is the table of comparison of analyzed packets in plain text and encrypted text of files of various sizes in Gmail.

Greater the analyzed packets, greater is the performance of the encrypted algorithm.

Table 2: Analyzed Packets-Elg-Gmail

Size	50kb	100kb	500kb	1mb	2mb
Plain text	225	295	776	1866	2612
Encrypted	119	113	114	222	252

Graph:

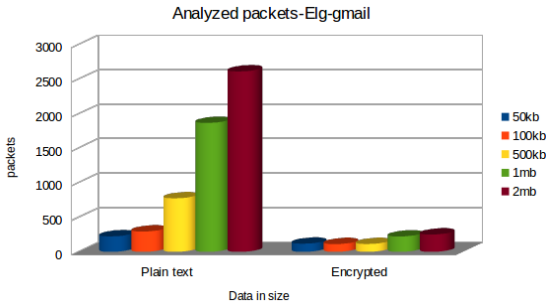

Fig 4: Analyzed Packets-ElGamal-Gmail

In the above graph the total number of analyzed packets remained consistent in encrypted text for corresponding plain text.

Run Time:

Run time is the total amount of time taken by Snort for analyzing the packets received from the Ethernet. If the run time taken during sending of plain text is higher when compared to encrypted text, then encrypting the text saves the processing time and memory. Following is the table of comparison of run time during sending plain text files and encrypted files.

Table 3: Run Time-ElGamal-Gmail

Size	50kb	100kb	500kb	1mb	2mb
Plain text	24.238	25.167	35.827	56.544	65.231
Encrypted	22.92	21.326	25.323	32.11	23.511

GRAPH:

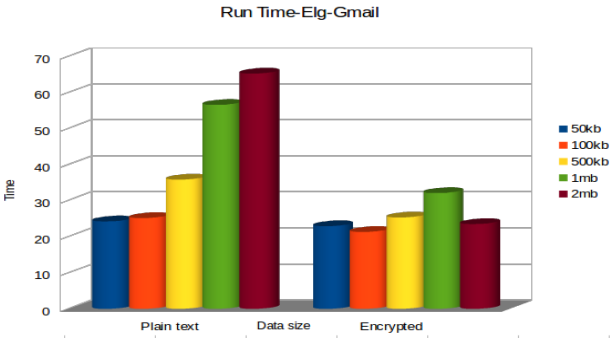

Fig 5: Analyzed Packets-ElGamal-Gmail

In the above graph the run time taken by SNORT for encrypted text is less when compared to plain text.

6.1.2 Applying ElGamal in Yahoo with SNORT.

Following is the table of analysis of data produced by SNORT when files are sent through Yahoo. The first row is the data of plain text sent when snort is running. The second row is the data of corresponding encrypted text using ElGamal encryption technique.

Total Packets: Total packets are the total number of packets received by the snort from the Ethernet.

Table 4: Total packets ElGamal-Yahoo

Size	50kb	100kb	500kb	1mb	2mb
Plain text	400	598	1041	2263	3241
Encrypted	324	368	584	244	314

GRAPH:

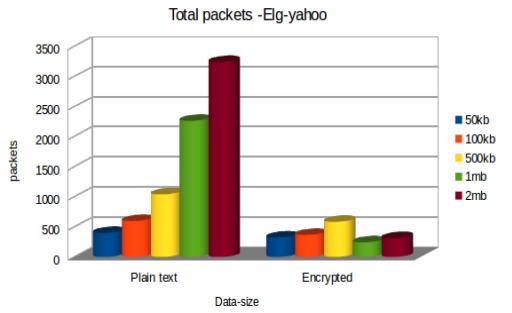

Fig 6: Total packets ElGamal-yahoo

In the above graph, encryption of the plain text by ElGamal technique reduced the number of total packets to considerably low, which saves a lot of time for processing.

Analyzed Packets:

Following is the table of comparison of analyzed packets in plain text and encrypted text of files of various sizes in Yahoo.

Table 5: Analyzed Packets-Elg-Yahoo

Size	50kb	100kb	500kb	1mb	2mb
Plain text	397	598	1041	2257	3223
Encrypted	319	368	569	235	307

GRAPH:

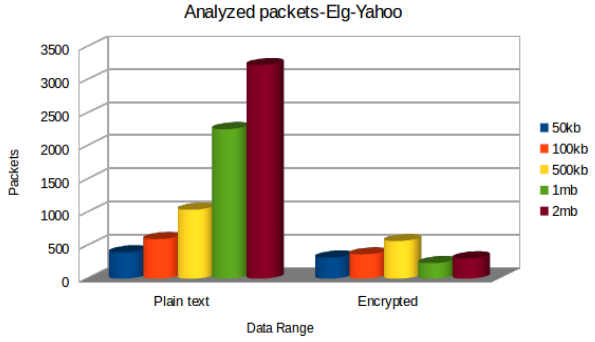

Fig 7: Analyzed Packets-ElGamal-Yahoo

In the above graph, the number of analyzed packets by SNORT was considerably low in encrypted due to the less number of total packets.

Run Time for analyzing packets:

Run time is the total amount of time taken by SNORT for analyzing the packets received from the Ethernet. If the run time taken during sending of plain text is higher when compared to encrypted text, then encrypting the text saves the processing time and memory.

Following is the table of comparison of run time during sending plain text files and encrypted files.

Table 6: Run Time -ElGamal-Yahoo

Size	50kb	100kb	500kb	1mb	2mb
Plain text	29.568	31.95	42.153	56.66	71.356
Encrypted	34.74	28.376	20.233	20.668	19.25

GRAPH:

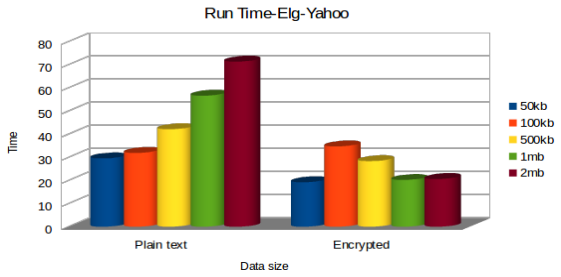

Fig 8: Run Time -ElGamal-Yahoo

In the above graph, the run time taken by encrypted text is more than plain text for 100kb size, which indicates that if file size is of 100 kb then sending the plain text saves us memory and time.

6.1.3 Applying ElGamal technique in Hotmail with SNORT

Following is the table of analysis of data produced by snort when files are sent through Hotmail. The first row is the data of plain text sent when snort is running. The second row is the data of corresponding encrypted text using ElGamal.

Total Packets:
Total packets are the total number of packets received by the SNORT from the Ethernet

Table 7 :Total packets-ElG-Hotmail

Size	50kb	100kb	500kb	1mb	2mb
Plain text	190	258	807	1788	2821
Encrypted	102	81	75	160	81

GRAPH

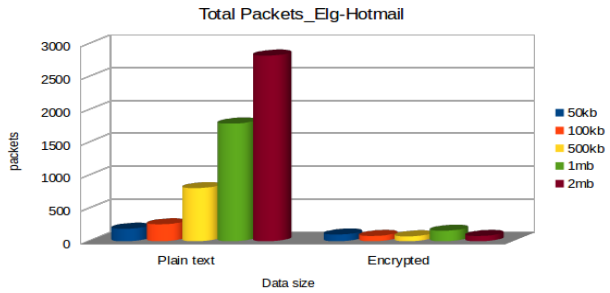

Fig 9: Total packets-ElGamal-Hotmail

In the above graph, the total number of packets produced by SNORT remained consistent irrespective of file sizes when compared to plain texts.

Analyzed Packets:

Following is the table of comparison of analyzed packets in plain text and encrypted text of files of various sizes in Hotmail.

Table 8: Analyzed Packets-ElG-Hotmail

Size	50kb	100kb	500kb	1mb	2mb
Plain text	190	258	796	1788	2475
Encrypted	102	81	75	149	81

GRAPH:

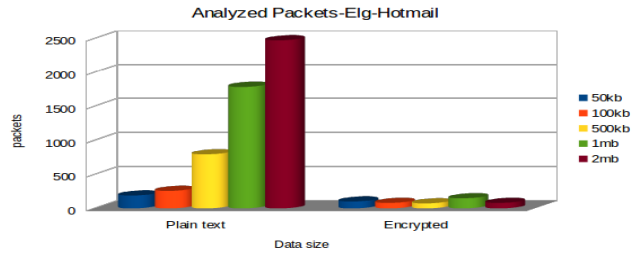

Fig 10: Analyzed Packets-ElGamal-Hotmail

In the above graph SNORT analyzed more number of packets for plain text when compared to encrypted text.

Run time:

Run time is the total amount of time taken by SNORT for analyzing the packets received from the Ethernet. If the run time taken during sending of plain text is higher when compared to encrypted text, then encrypting the text saves the processing time and memory.

Following is the table of comparison of run time during sending plain text files and encrypted files.

Table 9: Run Time-ElGamal-Hotmail

Size	50kb	100kb	500kb	1mb	2mb
Plain text	28.483	22.822	31.156	55.52	60.925
Encrypted	17.35	15.52	14.55	16.47	18.798

GRAPH:

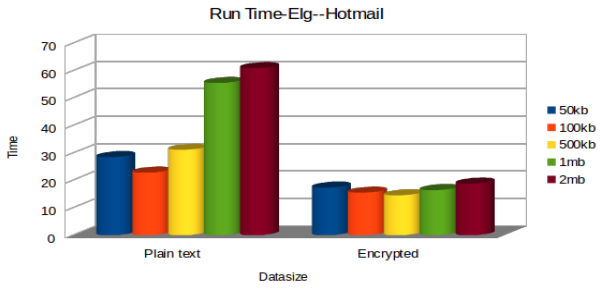

Fig 11 : Run Time-ElGamal-Hotmail

In the above graph run time taken by SNORT through Hotmail is higher for plain text when compared to encrypted text.

6.2 SNORT with RSA Technique

In this project, an experiment been carried out to analyze the data produced by SNORT during sending files(both plain text and encrypted text individually) of various sizes (50kb, 100kb, 500kb, 1mb, 2mb) in Gmail, Yahoo and Hotmail mail clients.

Initially the un-encrypted files are sent and the data produced by SNORT is compared to the data of encrypted files produced by SNORT.

Applying RSA Technique in Gmail with SNORT

Following is the table of analysis of data produced by SNORT when files are sent through Gmail. The first row is the data of plain text sent when snort is running. The second row is the data of corresponding encrypted text using RSA algorithm.

Total Packets:

Total packets are the total number of packets received by the SNORT from the Ethernet.

Table 10: Run Time-ElGamal-Hotmail

Size	50kb	100kb	500kb	1mb	2mb
Plain text	225	295	776	1870	2835
Encrypted	166	155	149	188	144

GRAPH:

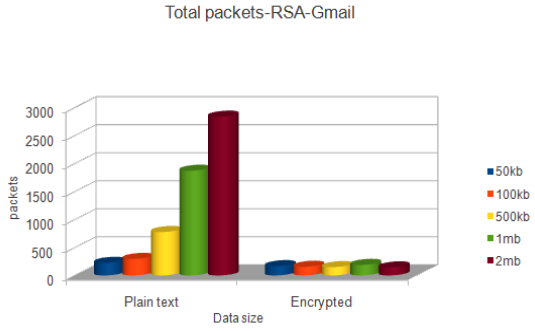

Fig 12: Total packets-RSA-Gmail

In the above graph the total number of packets analyzed by SNORT using RSA algorithm is consistent when compared to number of packets in plain text.

Analyzed Packets:
Analyzed packets are the packets analyzed by snort during runtime. SNORT doesn't analyze all the packets received by the Ethernet, it drops some of the packets that are needed to be buffered for processing.

Following is the table of comparison of analyzed packets in plain text and encrypted text of files of various sizes in Gmail. Greater the analyzed packets, greater is the performance of the encrypted algorithm.

Table 11: Analyzed packets-RSA-Gmail

Size	50kb	100kb	500kb	1mb	2mb
Plain text	225	295	776	1866	2612
Encrypted	119	113	114	222	252

GRAPH:

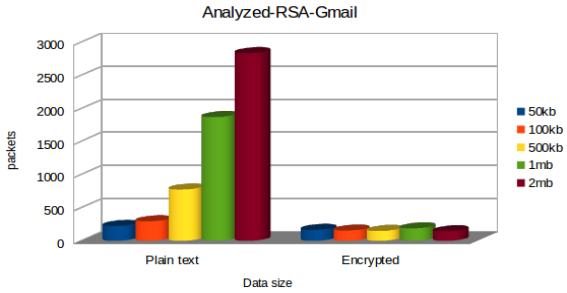

Fig 13: Analyzed packets-RSA-Gmail

In the above graph the number of packets analyzed by SNORT for encrypted is less when compared to plain text.

Run Time:
Run time is the total amount of time taken by SNORT for analyzing the packets received from the Ethernet. If the run time taken during sending of plain text is higher when compared to encrypted text, then encrypting the text saves the processing time and memory.

Following is the table of comparison of run time during sending plain text files and encrypted files.

Table 12: Run Time -RSA-Gmail

Size	50kb	100kb	500kb	1mb	2mb
Plain text	24.238	25.167	35.827	56.544	65.231
Encrypted	21.11	24.1	24.276	31.619	26.29

GRAPH:

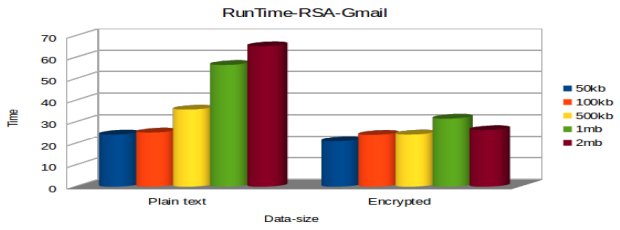

Fig 14: Table: Run Time -RSA-Gmail

In the above graph the total run time taken by SNORT for encrypted text is less when compared to plain text.

Applying RSA in Yahoo with SNORT
Following is the table of analysis of data produced by SNORT when files are sent through Yahoo. The first row is the data of plain text sent when SNORT is running. The second row is the data of corresponding encrypted text using RSA encryption technique.

Total Packets:
Total packets are the total number of packets received by the SNORT from the Ethernet

Table 13: Total packets-RSA-Yahoo

Size	50kb	100kb	500kb	1mb	2mb
Plain text	400	598	1041	2263	3241
Encrypted	372	451	445	168	368

GRAPH:

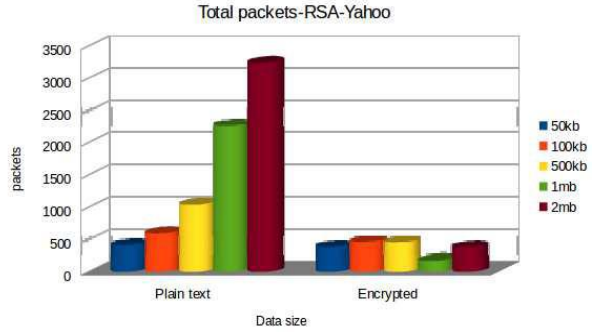

Fig 15: Total packets-RSA-Yahoo

In the above graph the total number of packets by SNORT for encrypted text is less when compared to plain text.

Analyzed Packets:
Following is the table of comparison of analyzed packets in plain text and encrypted text of files of various sizes in Yahoo.

Table 14: Analyzed Packets -RSA-Yahoo

Size	50kb	100kb	500kb	1mb	2mb
Plain text	397	598	1041	2257	3223
Encrypted	364	449	421	154	361

GRAPH:

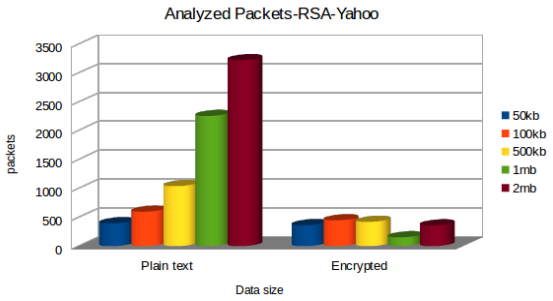

Fig 16: Analyzed Packets -RSA-Yahoo

In the above graph the number of analyzed packets by SNORT remained same in both plain text and encrypted text for 50 kb file size, but for other file sizes the number variation is higher.

Run Time:

Run time is the total amount of time taken by SNORT for analyzing the packets received from the Ethernet. If the run time taken during sending of plain text is higher when compared to encrypted text, then encrypting the text saves the processing time and memory.

Following is the table of comparison of run time during sending plain text files and encrypted files.

Table 15: Run Time-RSA-Yahoo

Size	50kb	100kb	500kb	1mb	2mb
Plain text	29.568	31.95	42.153	56.66	71.356
Encrypted	25.93	25.726	22.8	29.987	24.57

GRAPH

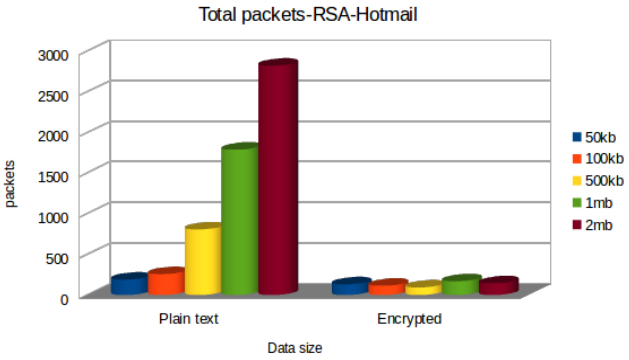

Fig 17: Run Time-RSA-Yahoo

Applying RSA technique in hotmail with SNORT

Following is the table of analysis of data produced by SNORT when files are sent through Hotmail. The first row is the data of plain text sent when SNORT is running. The second row is the data of corresponding encrypted text using RSA.

Total Packets:

Total packets are the total number of packets received by the SNORT from the Ethernet.

Table 16: Total packets-RSA-Hotmail

Size	50kb	100kb	500kb	1mb	2mb
Plain text	190	258	807	1788	2821
Encrypted	132	115	94	169	144

GRAPH:

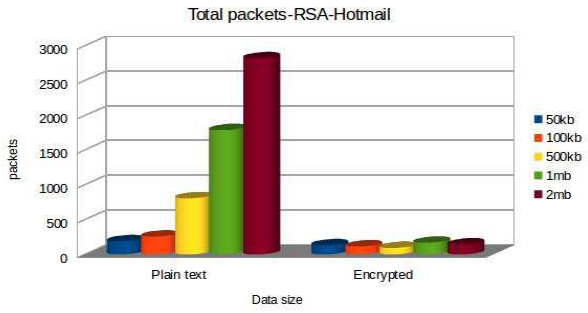

Fig 18: Total packets-RSA-Hotmail

In the above graph the number of packets received by SNORT for encrypted text remained consistent irrespective of the file size.

Analyzed Packets:

Following is the table of comparison of analyzed packets in plain text and encrypted text of files of various sizes in Hotmail

Table 17: Analyzed Packets -RSA-Hotmail

Size	50kb	100kb	500kb	1mb	2mb
Plain text	190	258	796	1788	2475
Encrypted	132	115	94	160	144

GRAPH:

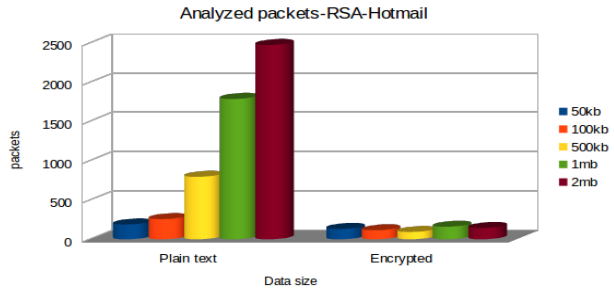

Fig 19: Analyzed Packets -RSA-Hotmail

In the above graph the number of packets analyzed by SNORT for encrypted text remained consistent irrespective of various sizes whereas it varied drastically for plain text.

Run time:

Run time is the total amount of time taken by SNORT for analyzing the packets received from the Ethernet. If the run time taken during sending of plain text is higher when compared to encrypted text, then encrypting the text saves the processing time and memory.

Following is the table of comparison of run time during sending plain text files and encrypted files.

Table 18: Run Time -RSA-Hotmail

Size	50kb	100kb	500kb	1mb	2mb
Plain text	28.483	22.822	31.156	55.52	60.925
Encrypted	19.923	18.357	18.77	22.932	20.343

GRAPH:

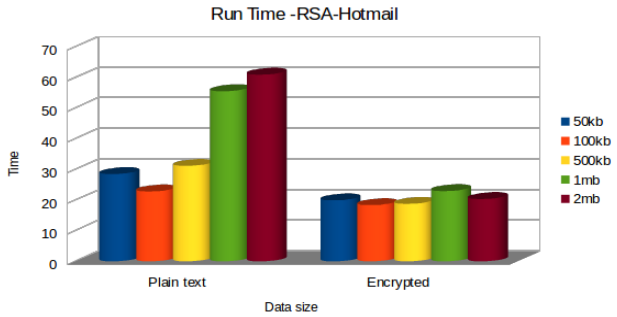

Fig 20: Run Time -RSA-Hotmail

In the above graph the run time taken by SNORT is less for encrypted text when compared to plain text.

7. CONCLUSION

In this paper, the performance of various mail clients like Gmail, Yahoo mail, Hotmail been analysed using free intrusion detection tool SNORT. Files ranging from 50 kb to 2 MB have been sent through all the three mail clients. It has been observed that while sending larger files Hotmail is having performance.

Then the same plain text files are encrypted using cryptographic algorithms like ElGamal and RSA and were sent through the same three mail clients. From simulation scenarios, it has been observed that encrypted files have shown high performance than plain text files. This has been proved with both RSA and ElGamal techniques

8. FUTURE ENHANCEMENT

In this paper, RSA and ElGamal algorithms have been experimented. There is still scope to extend these experiments with other algorithms for encryption.

9. REFERENCES

[1] G. Varghese, "Network Algorithmic: An Interdisciplinary Approach to Designing Fast Networked Devices", San Francisco, CA: Morgan Kaufmann, 2005.

[2] J. Cleary, S. Donnelly, I. Graham, "Design Principles for Accurate Passive Measurement," in Proc. PAM 2000 Passive and Active Measurement Workshop (Apr. 2000).

[3] A. Dabir, A. Matrawy, "Bottleneck Analysis of Traffic Monitoring Using Wireshark", 4th International Conference on Innovations in Information Technology, 2007, IEEE Innovations '07, 18-20 Nov. 2007,

[4] S. Ansari, Rajeev S.G. and Chandrasekhar H.S, "Packet Sniffing: A brief Introduction", IEEE Potentials, Dec 2002- Jan 2003, Volume:21, Issue:5, pp:17 – 19

[5] Daiji Sanai, "Detection of Promiscuous Nodes Using ARP Packet", http://www.securityfriday.com/

[6] Ryan Spangler , Packet Sniffer Detection with AntiSniff, University of Wisconsin – Whitewater, Department of Computer and Network Administration, May 2003

[7] Zouheir Trabelsi, Hamza Rahmani, Kamel Kaouech, Mounir Frikha, "Malicious Sniffing System Detection Platform", Proceedings of the 2004 International Symposium on Applications and the Internet (SAINT'04), IEEE Computer Society

[8] Hornig, C., "A Standard for the Transmission of IP Data grams over Ethernet Networks", RFC-894, Symbolic Cambridge Research Center,April 1984.

[9] Lin Tan, Timothy Sherwood. A High Throughput String Matching Architecture for Intrusion Detection and Prevention, Proceedings of the 32 nd Annual International Symposium on Computer Architecture (ISCA 2005).

[10] S. Mrdovic, E. Zajko. Secured Intrusion Detection System Infrastructure, University of Sarajevo/Faculty of Electrical Engineering, Sarajevo, Bosnia and Herzegovina (ICAT 2005).

[11] Yeubin Bai, Hidetsune Kobayashi. Intrusion Detection Systems: technology and Development, 17 th International Conference of Advanced Information Networking and Applications, (AINA 2003).

[12] Sang-Jun Han and Sung-Bae Cho. Combining Multiple Host-Based Detectors Using Decision Tree, Australian Joint Artificial Intelligence Conference, (AUSAI 2003).

[13] Ramaprabhu Janakiraman, Marcel Waldvogel, Qi Zhang. Indra: A peer-to-peer approach to network intrusion detection and prevention, Enabling Technologies: Infrastructure for Collaborative Enterprises, WET ICE 2003.

[14] M. Laureano, C. Maziero1, E. Jamhour. Protecting Host-Based Intrusion Detectors through Virtual Machines, The International Journal of Computer and Telecommunications Networking (2007).