HEAVEN'S LIGHT IS OUR GUIDE

RAJSHAHI UNIVERSITY OF ENGINEERING & TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

TITLE :

A STUDY ON DATA SECURITY AND DATA USAGE REGARDING ONLINE SERVICES

BY:

MD.YAMIN HAQUE(1603007)

MD AL SIAM(1603008)

OUTLINE

- CRYPTOGRAPHY
- ENCRYPTION ALGORITHMS
- DIFFERENT TYPES OF ATTACKS
- DATA BREACHES HISTORY

INTRODUCTION

- There have been established a wide range of service providing companies which are internet based.
- Giant companies can follow and track their user's activities and collects data on user's behaviors, movements, social relationships, interests, weaknesses and most private moments.
- As online services industry is growing bigger day by day, cyber attacking on data of all kinds of companies has increased. According to the National Cyber Security Alliance 60 percent of small and midsized businesses that are hacked go out of business within six months
- Security of data has become a major concern for both the company itself and the users

CRYPTOGRAPHY

IN CRYPTOGRAPHY IS THE ART OF SCIENCE OR COLLECTION OF TECHNIQUES OR TOOLS USED TO PROTECT THE DATA AND INFORMATION DURING ITS TRANSMISSION OVER THE NETWORK . IT INVOLVES ENCRYPTION AND DECRYPTION OF MESSAGES. ENCRYPTION IS THE PROCESS OF CONVERTING A PLAIN TEXT INTO CIPHER TEXT AND DECRYPTION IS THE PROCESS OF GETTING BACK THE ORIGINAL MESSAGE FROM THE ENCRYPTED TEXT

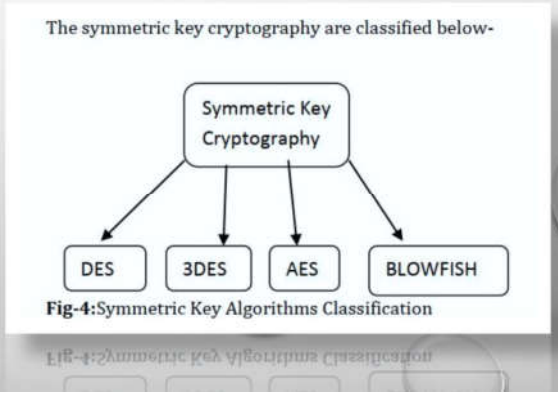

Fig-4: Symmetric Key Algorithms Classification

ENCRYPTION ALGORITHMS

	Symmetric Encryption Algorithms			
	DES	*TDES*	*AES*	*BLOWFISH*
Block Size	64 bit	64 bit	128 bit	64 bit
Key size	56 bit	168 bit	128,192, 256 bit	32-448 bit
Created By	IBM in 1975	IBM in 1978	Joan Daeman in 1998	Bruce Schneier in 1998
Algorithm Structure	Fiestel Network	Fiestel Network	Substitution Permutation Network	Fiestel Network
Rounds	16	48	9,11,13	16
Attacks	Brute Force Attack	Theoretically possible	Side Channel Attacks	Not Yet

DIFFERENT TYPES OF ATTACKS

- **SECURITY THREATS**
- **VIRUS ASSAULT**
- **UNAUTHORIZED APPLICATION INSTALLATION**
- **DATA STEALING AND CRYPTOGRAPHY ATTACKS**

DATA BREACHES

A **DATA BREACH** IS A CONFIRMED INCIDENT IN WHICH SENSITIVE, CONFIDENTIAL OR OTHERWISE PROTECTED **DATA** HAS BEEN ACCESSED AND/OR DISCLOSED IN AN UNAUTHORIZED FASHION. **DATA BREACHES** MAY INVOLVE PERSONAL HEALTH INFORMATION (PHI), PERSONALLY IDENTIFIABLE INFORMATION (PII), TRADE SECRETS OR INTELLECTUAL PROPERTY.

DATA BREACHES HISTORY

- **OVER 14,717,618,286 DATA BREACHES HAVE BEEN LOST OR STOLEN SINCE 2013.**
- **3,353,178,708 RECORDS WERE COMPROMISED IN THE FIRST HALF OF 2018.**
- **86% OF ALL BREACHES IN 2017 OCCURRED IN NORTH AMERICA.**
- **IN 2018, 45.9% OF DATA BREACHES IN THE US WERE IN THE BUSINESS SECTOR.**
- **IN JANUARY 2015, A RUSSIAN HACKER CALLING HIMSELF "PEACE" STOLE 117 MILLION LINKEDIN EMAIL AND PASSWORD COMBINATIONS.**
- **CRAFTY CYBERCRIMINALS MANAGED TO COLLECT THE PERSONAL DATA OF OVER 500 MILLION GUESTS OF THE MARRIOTT INTERNATIONAL HOTEL CHAIN BETWEEN 2014 AND 2018.**
- **IN SEPTEMBER 2018, A SUCCESSFUL ATTACK ON FACEBOOK COMPROMISED 50 MILLION USER ACCOUNTS.**

HOW COMPANIES USE USER DATA

ONLINE SERVICES HAS A BIG COLLECTION OF DATA TO MAKE BENEFITS FOR EVERYONE IN MANY AREAS OF LIFE. BUT COMPANIES AND OTHER INSTITUTIONS CAN EASILY USE THEIR DATA WEALTH AGAINST PEOPLE. THE POSSIBLE ADVERSE EFFECTS OF CORPORATE DATA COLLECTION AND UTILIZATION ON INDIVIDUALS, GROUPS OF PEOPLE, AND SOCIETY ARE DIVERSE, BUT RARELY CONSIDERED IN THE COMMERCIAL SPHERE.

CONCLUSION

BASICALLY, THIS PAPER FOCUSED ON BIG COMPANIES OR INSTITUTION WHO HAVE A VAST AMOUNT OF USER PROFILE OF PEOPLE ALL AROUND THE WORLD. IN THIS PAPER, STUDY ON DIFFERENT TYPES OF ENCRYPTION TECHNIQUES IS DONE. SOME DATA BREACHES INCIDENTS HAPPENED SO FAR HAVE BEEN STUDIED ALSO. LATER, HOW COMPANIES USE USER DATA IS EXPLORED. COMPANIES USE DATA TO GIVE BETTER SERVICES AS WELL AS TO BIAS AND CLASSIFY USERS.