RESEARCH ARTICLE OPEN ACCESS

Analysis of Cryptographic Hash Functions and Cryptographic Technique

[1]**RASHMI RANJAN SETHY,**
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]**SUBHRANSHU RANJAN JENA,**
Shibani Institute of Technical Education, Bhubaneswar, Odisha, India

ABSTRACT: We begin with the fundamentals of cryptography before moving on to its development. The focus is primarily on different algorithms, such as DES and RSA. Additionally, we explored the families of MD, SHA, RIPEMD, BLAKE, and WHILPOOL cryptographic hash functions here. Finally, we concluded the paper comparison.
Keywords:DES, AES, RSA, Hash Function,MD5,SHA3,BLAKE,RIPEMD,WHIRLPOOL

I. INTRODUCTION

CryptographyItistheprocessoftransformingthesecretdataorinformationintoaunreadable or scrambled form.In fact it is the art of writing the message secretly. Theconceptofcryptographydependson fivefactors.Thesearediscussedbelow[1]

(a) **Plain text:** The message or information that we want to send secretly. The set of plain text isrepresented by**P**.

(b) **Cipher text:** It is the scrambled or unreadable form of information or message. The set ofciphertext is representedby**C.**

(c) **Key:**Itistherulewiththehelpofwhichdataisscrambled.Thesetofkeysisrepresentedby **K.**

(d) **EncryptionFunction:**Itisthemethodusing whichtheciphertextisgenerated.Thesetofencryptionfunction is represented by**E(x)**.

(e) **DecryptionFunction:**Itistheinversefunctionof E(x).Itistheefforttogeneratetheoriginalmessage. Theset of decryptionfunctionis represented by**D(x)**.

Thuscryptographyisdependson {**P,C, K,E(x), D(x)**}

CryptographyGoal

Cryptographicgoalsare setbeforedevelopinganewencryptionmodel.

- AccessControl
- Authentication
- Confidentiality
- Data Integrity
- Non-Repudiation

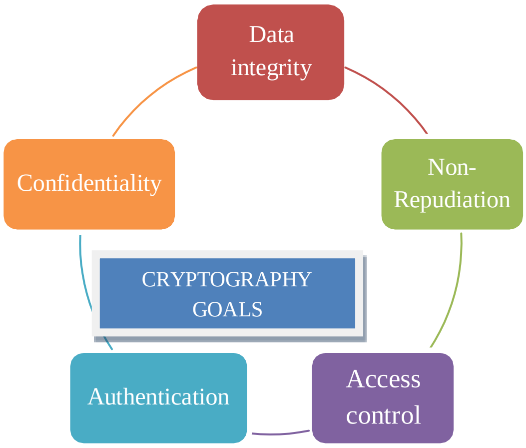


Figure1:Cryptographygoals

TypesofKeys

- SymmetricKeyCryptography
- Asymmetric KeyCryptography

It is a two key system also known as the public key system, one key encrypts the informationandanother,andmathematicallyrelatedkeydecryptsit. RSAalgorithmisonesuchexample.

II. HISTORY OF CRYPTOGRAPHY

It is considered that as people become able to write the art of cryptography was born alongwith it. With the time, human beings got organized in kingdoms, tribes and groups. Thenideas suchas politics,battles, power evoke the natural need of people to communicatesecretly. Thus journeyofcryptographybegins.

Hieroglyph

Some4000yearsago,thetechniquenamed**Hieroglyph**wasusedbytheEgyptianstocommunicate secret messages within the scribes. It was known to be the oldest cryptographictechnique. This secret code was only available with the person who used to deliver messageonthe behalf oftheking.

CaesarShiftCipher

ThencametheRomanmethodofcryptography.EachalphabetofEnglishlanguageisassociatedto aspecificnumberand performs accordingly.Substitution isshown below

A→0	B→1	C→2	D→3	E→4
F→5	G→6	H→7	I→8	J→9
K→10	L→11	M→12	N→13	O→14
P→15	Q→16	R→17	S→18	T→19
U→20	V→21	W→22	X→23	Y→24
Z→25				

Figure2:Substitutionmatrix

Mathematically,wedefinea
E(x):L→Z26
whereListhesetoflettersi.e.,
Lettheencryptionfunctionbe
………..(1)PlainText:

D A U G H T E R
Position:
3 0 20 6 7 19 4 17
(Substitution bynumbers)

Key:
6 6 6 6 6 6 6 6

E(x):

9 6 26 12 13 25 10 23 (Result)

E(x):
9 6 1 12 13 25 10 23
(Replace 26by1)
CipherText:

J G B M N Z K X
(encodedmessage)
i.e., the word **DAUGHTER** is encrypted as **JGBMNZKX** under the function E. Now, wehave to decode the message, for this we need to define another function i.e., decryptionfunctionwhich is theinversefunction of(1)
Thedecryption functionis givenby
– (2)CipherText:
J G B M N Z K X
(encodedmessage)

E(x):
9 6 1 12 13 25 10 23
Key:

6 6 6 6 6 6 6 6

(Subtractingthekey)

D(y):

3 0 -5 6 7 19 4 17

E(x)

3 0 6 7 19 4 (Replace-5 by20)
20
17
Originalmessage:
D A U G H T E R

Inthiswaythereceivergetstheoriginalmessageusingdecryptionfunctiondependinguponsamekey.

Shortcomings:
(a) Searchspaceisverysmall,eachletterhasonly 25shiftsbesidesitself.Onlyalittlepatienceoftryingall the possibilities will revealthemessage
(b) Aseveryletterisshiftedbyafixednumber,ifw eabletodeterminethedecryptionofonethenweareable to decodethe entiremessage.

SubstitutionCipher

Later,during500to600BCthescholarsevolvedsimplemono-alphabeticsubstitutionciphers. It replaces one character of plaintext with other symbol or character by using somerule.Thisruleusedtogetbackthemessage.Asubstitutioncipherishardertobreak.Thewaythis oneworks is wemap eachalphabet to anotheralphabetin theletter.

Shortcomings: Search space is very small, spending reasonable time on searching for resultstheattackergets thesolution easily.

AffineCipher

P =={0, 1, 2, 3,.., 25}

.Length ofkey=2

MathematicalModeling:

ForExample **:**Consider keyk=(15,18) clearlygcd(15,26)=1

VigenereCipher

Animprovedcipher**vigenerecipher**cameintoexistenceinthe15th centuryandwasfirstpublished in1863

Plaintext:MEE TIN GA TNIN EKey:LIG H TLIG HTLIG

Ciphertext:XM KAB YOG AGTVK

Here,keyisthewordLIGHT.Infigure3rowsrepresents theplaintextwhereascolumnsrepresentsthekeyand thecells represents theencrypted transformations.

Shortcomings: The repeating nature of the key is the major problem with this cipher .If theguessforkey's lengthsetscorrectthen themessageiseasilydecryptedbythe attacker.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure3:VigenereTable

HillCipher

In 1929, Lester S. Hill gives new dimensions to cryptography by introducing the usage oflinear algebra to scramble the plain text. He used familiar concepts like matrix multiplicationand inverse of matrix for encryption and decryption. In this method the key is a n x ninvertiblematrix.

Shortcomings: As the Hill cipher is completely linear so an attacker can set up a linearsystemwhichcanbeeasily solved.Calculating thissolutionby standardlinearalgebraalgorithmsthen takes verylittle time.

III. FAMOUS ALGORITHMS

RSA

It is the system in which part of the Key made public by the receiver and part of key leftsecrect.Publickeyused for encryptionand secret/Private keyis usedfordecryption.

Publickey cryptosystem	KeySpace(Public ,Private)	Encryption	Decryption
RSA	{(| Public=(n,e),Private =(p,q,d)		

BlockCipher
- SupposeAliceandBobwant touseblockcipherforencryption.
- Theyagreedon blockcipher.
- SupposeAlicehas longmessageof m bits.
- SupposeAliceandBobhave‘L’bitblockcipher(DES-64bit,TripleDES-64bit,AES-128bit, SPN)with key.
- Longmessage‘m‘willbebroken‘L’bitblocks,inthelastblocksomedummybitswillbeappended tomakeitLbit[3].

AdvancedEncryptionStandard(AES)

- EarlierCiphers(Classical)brokenundertheifwehavethemoderncomputerspeed.Notsecure.
- IfwehavetheDESwhichisalsobrokenby thegenericattack,timetradeoffattack,Exhaustive searchAttack
- OnDESonecanmounttheNon-genericattacklikedifferentialcryptanalysisattack ,linearcryptanalysisattack .DES is not secure.
- Weneed tohave alternatestandard, wehaveTriple DES, 3X16=48rounds , sohuge.
- AES is designed to resist the generic ,Differential and linear cryptanalysis attack and all otherexistingattacks[5,12].

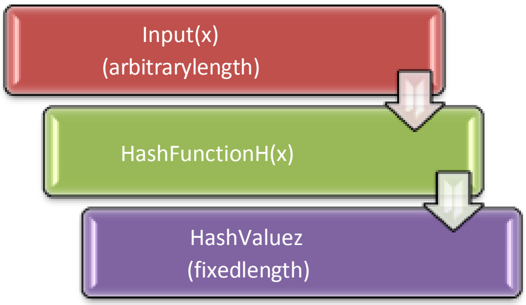
Table2:ComparisonbetweenStandardAlgorithms

NameofAlgorithm	**Origin**	**Keytype**	**Createdby**	**Year**	**KeySize(inbits)**	**Blocksize(inbits)**	**Rounds**	**Shortcomings**
DES[3]	Lucifer	Symmetrickey	IBM	1975	56	64	18	Not deemed sufficient to encrypt sensitivedata

3DES	DES	Symmetrickey	IBM	1978	112 or 168	64	48	Slow
AES	Square	Symmetrickey	Joan Daemenand VincentRijmen	1998	128, 192, 256	128	10,12,14	PowerAnalysisAttack
RSA	Mathematical,basedonproduct oflargeprimes	Asymmetric key	**R**ivest**S**hamir**A**delman	1977	1024 to 4096		1	Difficult todecide largep and q(slowest)

IV. CRYPTO GRAPHIC HASH FUNCTION

It is the one of the Mathematical functions where hardness lies in finding the inverse. Outputof



the hash functions is of fixed length irrespective of length of input numerical message.Suchoutput of fixed length is called messagedigest [4].

4.1PropertiesofHashFunctions

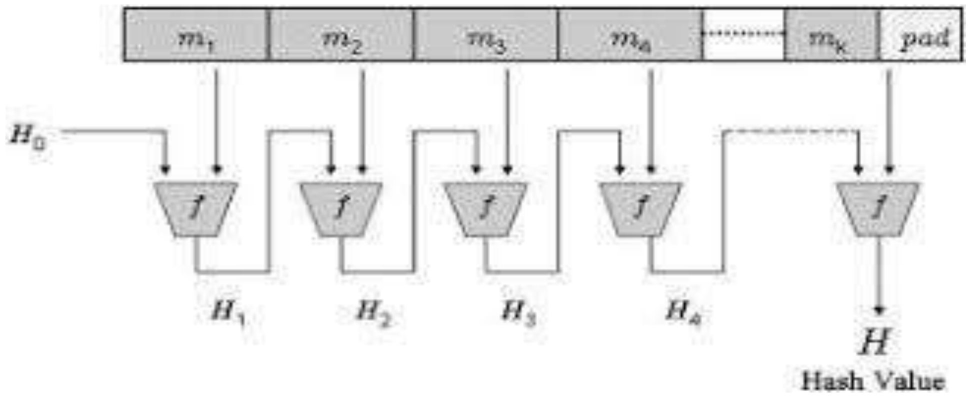
Itshouldbeappliedtoanysizeinput andproduce fixed lengthoutput.
H(x),thehashfunctionhasthefollowingmathematical properties:

(a) Pre-ImageResistance(Hardtoreversethefunctionalvalue)
Let x be the input and z be the hash value which is produced using the hash function, i.e.,H(x)=z then $H^{-1}(z)$=xis difficultto compute.Itmeanscomputationallyinfeasible
Itsecurefromanattacker havingonlyoutputvalue of hashfunction.

(b) SecondPre-Image Resistance(Hardnessinfindingequalvalueofgiven hashvalue)
s.t..

(c) Collision Resistance (Different inputs but same output) Let be two different input values and exists but the conditionishard to develop [6].

<u>GeneralStructureof HashFunction:</u>
,BigmessageM divided intoblocks each.



V. SOME HASH FUNCTIONS

1) **MessageDigest(MD):**Therearevarioushashfunctionsdevelopedinthiscategorylike MD2,MD4, MD5 and MD6[7].

2) **RIPEMD(RaceIntegrityPrimitiveEvaluation MessageDigest):**Openresearchcommunityhaddeveloped thesetypeoffunctions.It includesRIPEMD160

3) **Whirlpool:**It512bitfunctionderivedfrom advancedencryptionstandard[14].

4) **SecureHashFunction(SHA):**Varioussecurehashfunctionsarepartofthisfamilylike SHA-3,SHA-2,SHA-1 and SHA-0 [10].

5) BLAKE

Family of **BLAKE** comprises of BLAKE, BLAKE 2, BLAKE 256, BLAKE 224, BLAKE384,BLAKE 512[13].

These are hash functions based on Dan Bernstein's ChaChastream cipher, but a permutedcopyof the input block, XORedwith some round constants, is added before each ChaCharound.

Like SHA-2, there are two variants differing in theword size. ChaCha operates on a 4×4array of words. BLAKE repeatedly combines an 8-word hash value with 16 message words,truncatingtheChaCharesult to obtain thenext hashvalue.

BLAKE-256 and **BLAKE-224** use 32-bit words and produce digest sizes of 256 bits and 224bits, respectively, while **BLAKE-512** and **BLAKE-384** use 64-bit words and produce digestsizes of 512 bits and 384 bits, respectively. When run on 64-bit x64 and ARM architectures,BLAKE2isfaster than SHA-3, SHA-2, SHA-1, and MD5.

Table2:ComparisonbetweenvariousHashFunctions

HashFunction	**Designer**	**Year**	**Structure**	**Attack**	**Attackyear**	**Outputsize**	**Blocksize /Rounds**
MD5	RonaldRivest	1992	Merkle-demgardconstruction	collisionsfound	2012	128	512
RIPEMD	Hansdobertin, AntoonBosselears,BartPreneel	1996	Based onMd4	Collision	2004	128 160 256 320	
WHIRLPOOL [11]	VincentRijmen,PauloS.L.M.Barreto	2000	Miyaguchipreneel	Reboundattack	2009	512	Round10

SHA2	Nationalsecurity Agency	2001	Merkle- damgard construction withdevies meyer compression function	Pre imageresistanceCollisionresistance	2011	224,256, 384, 512	256,(8 x 32),512 (8 x64)
SHA 3(KECCAK)	GuidoBertoni, Joan daemen,Micheal	2012	SpongeConstruction	Collisionsfound		224, 256,	1152 1088
[9]	Peeters, GillesvanAssche					384, 512	832 576
BLAKE	Jean-Philippe Aumasson,Luca Henzen, WilliMeier, Raphael C.-W. Phan	2012	HAIFA Construction	-----	------	224, 256, 384, 512	Rounds (14,16)

VI. CONCLUSION AND FURTHER RESEARCH

This paper gives the comparisons between various cryptographic algorithms and differenthash functions which help to understand the crux of cryptography. In various hash functionattackswerefound.Moreeffectiveattackscan bedevelopi.e.,thesecuritylevelofnewlyandeffectively develop hash functions can bechecked.

REFERENCES

[1]. AtulKahate“CryptographyandNetworkSecurity”,TataMcGraw-HillCompanies,2008
[2]. D. Boneh and M. Franklin, “Identity-based encryption form the weil pairing”, in Advance inCryptology(CRYPTO’01),LNCS2139, SpringerVerlag,37, 213-229,2011
[3]. Davis.R, “The Data Encryption Standard in Perspective”, Proceeding of CommunicationSocietymagazine,IEEE,Vol 16, Nov1978
[4]. Mr. Gurjeevan Singh, Mr. AshwaniSingla and Mr. K S Sandha, "Cryptography AlgorithmComparisonforSecurityEnhancementinWirelessIntrusionDetectionSystem",InternationalJournalof MultidisciplinaryResearch, Vol.1Issue4,pp. 143-151,August2011.
[5]. Zilhaz Jalal Chowdhury, DavarPishva and G. G. D. Nishantha, “AES and ConfidentialityfromtheInsideOut”,the12thInternationalconferenceonAdvancedCommunicationTechnology(ICACT), pp.1587-1591,2010.
[6]. https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm
[7]. Xiaoyun Wang; DengguoFeng; Xuejia Lai; Hongbo Yu (2004-08-17). "Collisions HashFunctionsMD4 MD5 RIPEMD HAVAL". Retrieved2017-03-03.
[8]. GuidoBertoni,JoanDaemen,MichaëlPeetersandGillesVanAssche."OntheIndifferentiabilityof the SpongeConstruction".EuroCrypt 2008.
[9]. KeccakimplementationoverviewVersion 3.2,section3.1
[10]. Hernandez,Paul(5August2015)."NISTReleases SHA-3CryptographicHashStandard".
[11]. Florian Mendel1, Christian Rechberger, Martin Schläffer, Søren S. Thomsen (2009-02-24).The Rebound Attack: Cryptanalysis of Reduced Whirlpool and Grøstl(PDF). Fast SoftwareEncryption:16thInternationalWorkshop.
[12]. Paulo S. L. M. Barreto (2008-11-25). "The WHIRLPOOL Hash Function". Retrieved 2017-03-03.

[13]. Saarinen, M-J; Aumasson, J-P (November 2015). The BLAKE2 Cryptographic Hash andMessage Authentication Code (MAC). IETF. doi:10.17487/RFC7693. RFC 7693. Retrieved 4December2015.
[14]. Joan Daemen and Vincent Rijmen, "The Rijndael Block Cipher," AES submission availableat:http://www.nist.gov/aes.