Cryptography library

Gabriel Jiménez B23466
Carla Vega B06763

University of Costa Rica

October 7th, 2013

Overview

1. Introduction
2. GEYKE93
    - AES
    - RSA
    - Hash function
        - MD5
        - SHA2
3. Libraries
    - Crypto++
    - Beecrypt
    - Hashlib++
4. Applications and protocols

History

- Julio César
- XV León Battista Alberti
  - 1470
  - 1530
- XVI Girolamo Cardano
- XIX Transposition
- 1919 Alexander Koch and Arthur Sherbius (ENIGMA) 1st patent
- 1975 Diffie and Hellman public key algorithms

Cryptology

Combined study of cryptography and cryptanalysis

- Cryptoanalysis: study of how to crack encryption algorithms or their implementations.
- Cryptography: use and practice of cryptographic techniques.
  - "hidden, secret"; and graphein, "writing".

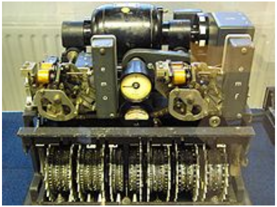
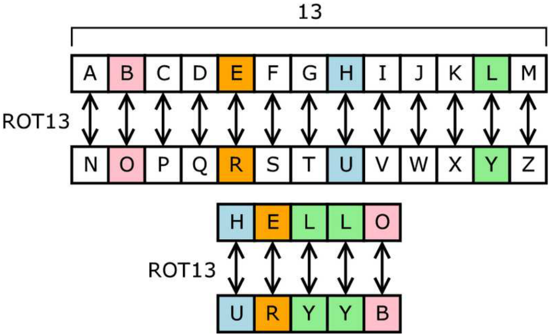


Figura: German Lorenz cipher machine

Classic criptography

- Sustitution: Cesar algorithm (A becomes D, B becomes C...), ROT13, ROT47, Vigénere
- Transposition: random order



13

ROT13

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

H E L L O

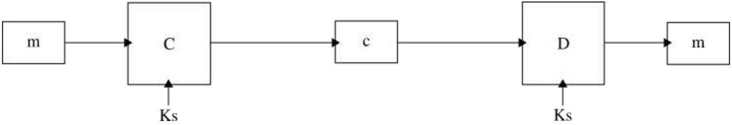
ROT13

U R Y Y B

Criptography algorithm

Simetric or convencional cryptosystem

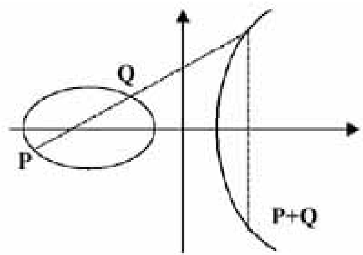
- Polyalphabetic Cipher: Enigma, Purple, SIGABA, TypeX
- Stream Cipher (Cifrado de flujo): RC4, Chameleon, FISH, Helix, ISAAC, Panama, Pike, SEAL, SOBER, WAKE
- Block Cipher: DES, AES, IDEA, Skipjack, Blowfish, RC2, RC5, CAST-128



Criptography algorithm

Asimetric or public key cryptosystem

- Diffie-Hellman
- RSA
- DSA (Digital signature algorithm)
- ElGamal
- ECC (Criptografía de curva elíptica)



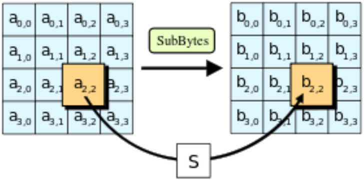
GEYKE93 contents

- AES
- RSA
- Hash function: MD5, SHA256, SHA512

AES

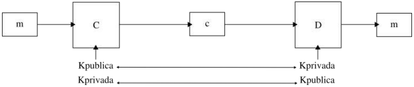
Advanced Encryption Standard

- Rijndael (Joan Daemen y Vincent Rijmen, Katholieke Universiteit Leuven)
- 1998
- Key sizes: 128, 192 or 256 bits
- Structure: Substitution-permutation network


$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
SubBytes
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
S

RSA

- Ron Rivest, Adi Shamir, Len Adleman (MIT, 1977)

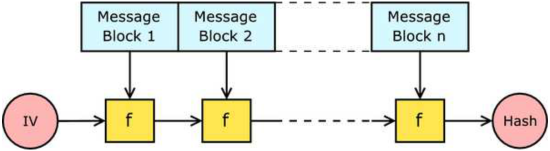


RSA

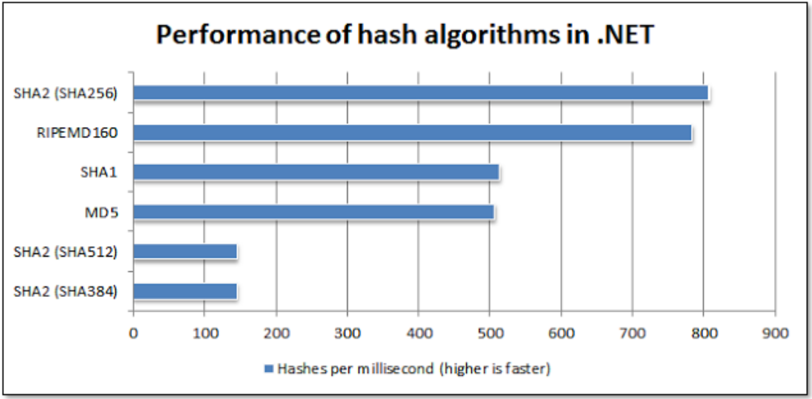
- (M, C, K, E, D)
- (C_i, D_i)
- $N = PQ$
- $f = \varphi(N) = (P-1)(Q-1)$
- E Euclides Algorithm (m.c.d)
- Public key (E, N)
- $DE \equiv 1 (modf)$
- Private key = D
- $C \equiv M^E (modN)$
- $M \equiv C^D (modN)$

Hash function

- Digital sign
- Fingerprint or digest
- Algorithm: HAVAL, MD2 (Message digest algorithm), MD4, MD5, SHA0, SHA1, SHA2, SHA3*, Snefru, Tiguer, Whirlpool



Hash function

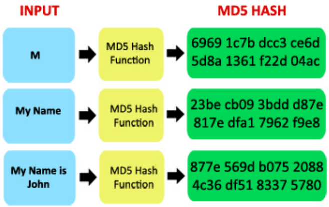


MD5

Message digest algorithm

- Produces a 128-bit (16-byte) hash value
- Ron Rivest (1991): replace an earlier hash function, MD4.
- MD5 hash value is typically expressed as a hexadecimal number, 32 digits long.
- Attack
  1. A 2009 attack by Tao Xie and Dengguo Feng breaks MD5 collision resistance in $2^{20,96}$ time. This attack runs in a few seconds on a regular computer.
  2. GPUs. Ex: NVIDIA GeForce 8400GS graphics processor, 16–18 million hashes per second can be computed and NVIDIA GeForce 8800 Ultra can calculate more than 200 million hashes per second.

MD5



INPUT

MD5 HASH

M → MD5 Hash Function → 6969 1c7b dcc3 ce6d 5d8a 1361 f22d 04ac

My Name → MD5 Hash Function → 23be cb09 3bdd d87e 817e dfa1 7962 f9e8

My Name is John → MD5 Hash Function → 877e 569d b075 2088 4c36 df51 8337 5780

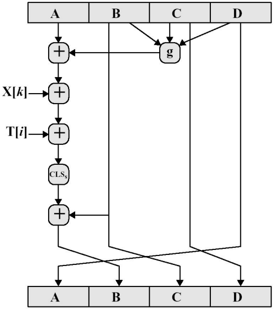


Figure 9.3 Elementary MD5 Operation (single step)

SHA2

- SHA0 160-bit hash function (1993).
- SHA1 National Security Agency (NSA) 2010.
- SHA2 National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS) 2001.
    - SHA256: 32-bit words
    - SHA512: 64-bit words
- Truncated versions of each standardized, known as SHA-224 and SHA-384 (NSA).
- SHA3 (Keccak, 2012) public competition among non-NSA designers. Same hash lengths as SHA2, and its internal structure differs significantly.

Crypto++

Crypto++

- Cipher: Panama, Sosemanuk, Salsa20, XSalsa20.
- MAC: VMAC, HMAC, GMAC, CMAC.
- Hash functions: SHA1, SHA2, SHA3...
- Public key cryptosystems: RSA, DSA, ElGamal
- KAS: DH, DH2, MQV, LUCDIF

Beecrypt

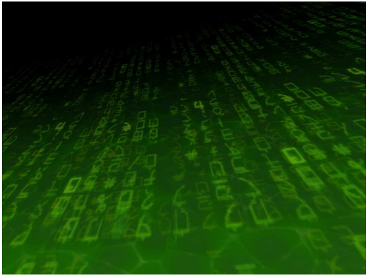
- Entropy sources, random generators, block ciphers, hash functions, message authentication codes, multiprecision integer routines, public key primitives...
- Highly optimized C, algorithms: Blowfish, MD5, SHA-1, Diffie-Hellman, and ElGamal.
- Free software.
- BeeCrypt for Java (JCE 1.2 crypto provider).

Hashlib++

- Library to create cryptographic checksum called "hashïn C++.
- hashlib++ is written in plain C++ and should work with every compiler and platform.
- It is released under the BSD-license and therefore free software. Copyright (c) 2007-2011 Benjamin Grüdelbach
- Hierarchy:
  - Hashwrapper: md5wrapper, sha1wrapper, sha256wrapper, sha384wrapper, sha512wrapper.
  - MD5
  - SHA1
  - SHA256
  - SHA2ext
  - Others

Applications

- GnuPG (GNU provacy guard) Free Software Foundation
- HTTPS (example: homebanking)
- GPG The GNU Privacy Guard (example: correo electrónico encriptado).
- PGP (Pretty good privacy) Phil Zimmerman



Protocols

- SSH (Secure Shell)
- DSS (Digital satellite system)
- SET (Secure electronic transaction)
- SSL (Secure sockets layer)
- TLS (Transport layer security)
- OpenPGP

SSH

SSH uses public-key cryptography to authenticate the remote computer and allow it to authenticate the user, if necessary.

- Use automatically generated public-private key pairs to simply encrypt a network connection, and then use password authentication to log on.
- Use a manually generated public-private key pair to perform the authentication, allowing users or programs to log in without having to specify a password.

SSH only verifies whether the same person offering the public key also owns the matching private key.

Acceptance and revision methods

Standard organizations

- ANSI (American National Standards Institute)
- ISO (International Organization for Standardization)
- IEEE (Institute of Electrical and Electronics Engineers)
- IETF (Internet Engineering Task Force)

Acceptance and revision methods

Criptograph organizations

- NSA (National Security Agency)
- GCHQ (Government Communications Headquarters) UK government
- Communications Security Establishment (CSE) Canadian intelligence agency.

- NESSIE (New European Schemes for Signatures, Integrity, and Encryption) (European Union)

NESSIE

- CrypToolproject (eLearning Program for Cryptography and cryptanalysis)

CrypTool

- CRYPT REC (Cryptography Research and Evaluation Committee) (Japanese Government)