Криптография

1. Основи на криптографията

- История и общи понятия
  Теория на Кодирането (Оптимално кодиране, шумозащитно кодиране, криптиране)
  Криптография/Криптоанализ
  cleartext/encoded data/key
  криптиране/електронен подпис
  циклични/блокови алгоритми
  SnakeOil/strong алгоритми
  Caesar's Cipher, Enigma/Ultra
  1927 Scherbius

- Симетрични криптоалгоритми (базирани на секретен ключ)
  схеми (криптиране/подпис)
  DES, 3DES, Blowfish, IDEA, Cast, RC2, RC4, RC5, FEAL, SAFER

- Асиметрични криптоалгоритми (базирани на публичен ключ)
  public/private key (криптиране на private ключа със симетричен)
  схеми (криптиране/подпис)
  RSA, DSA, ElGamal, Diffie-Hellman, Eliptic Curves

- Hash функции
  схеми
  MD4, MD5 (128 бита), SHA1 (168 бита), RIPEMD-160
  one-way функции
  приложение: в симетричните/асиметричните криптоалгоритми, консистентност на данните, пароли
  UNIX crypt = [password] -> модифициран DES в/у 64 zero bits -> [hash]

2. Преглед. Криптографски алгоритми, имплементации, протоколи.

- Принцип на работа на DES (Data Encryption Standart)
  разработен от IBM, приет за стандарт от NBS (национално бюро
  по стандартите) през 1967, през 1980 приет от ANSI (FIPS 46-2)
  блокове от по 8 байта / ключ с ефективна дължина 56 bita (реални 64 bits - 8,16..64 - parity)
  (72 057 594 037 927 946 комбинации, криптоанализ - 16 000 000)

  64bit -> пермутация -> L0 R0 (16 цикъла)

```
L(i)=R(i-1)
R(i)=L(i-1) XOR f( R(i-1), K(i) )
f = {
[R(i-1)] -32-> [Expander 32/48] -48-> [XOR K(i) /48/] ->
-48-> {
      /6/   S1    /4/
      /6/   S2    /4/
            ...
      /6/   S8    /4/
       } -32-> [пермутация] -32->
}
```

  S - таблици на субституциите
  Ki - серия от пермутации и SHL на оригиналния ключ
  DES дефинира конкретните пермутации, S-таблиците, и т.н.

- Принцип на работа на RSA

  Diffie-Hellman 1976 "Нови насоки в криптографията", PKS D(E(P))=P
  Rivest, Shamir, Adleman 1978 "Един метод за получаване на цифрови
  подписи и системи с публичен ключ"

  a) random големи прости числа p и q от приблизително един и същи порядък
  b) n = p * q
  c) random голямо число D, взаимнопросто със (p-1)*(q-1)
  d) изчислява се E, така че (E*D) mod ((p-1)*(q-1)) = 1
  e) public key - (E,n), private key (D,n)

f) входните данни се разделят на блокове, които могат да се представят като числа в интервала [0, n-1]
g) A ^ E mod n = B
B ^ D mod n = A

пример:
p = 3
q = 11
n = p*q = 33
(p-1)*(q-1) = 20
нека D = 7 (взаимнопросто с 20)
нека E = 3 (3*7 mod 20 = 1)
public = (3,33)
private = (7,33)

```
        |   ^3 | mod 33 ||          ^7 | mod 33
-----------------------------------------------
R = 18 | 5832 |     24 ||  4586471424 |     18
S = 19 | 6859 |     28 || 13492928512 |     19
A =  1 |    1 |      1 ||           1 |      1
```

намиране на прости числа:
Сито на Ератостен
Ойлерово обобщение на Малката теорема на Ферма
P - просто
X - не е кратно на P
X ^ (P-1) mod P = 1
Квадратично сито
Сито на числовото поле
длъжина на ключа
RSA-129 (17 години)
155 = 512bits

Reference		Magnitude
Seconds in a year		3E+7
Age of our solar system (years)		6E+9
Seconds since creation of solar system		2E+17
Clock cycles per year, 50 MHz computer		1.6E+15
Binary strings of length 64	2^64	1.8E+19
Binary strings of length 128	2^128	3.4E+38
Binary strings of length 256	2^256	1.2E+77
Number of 75-digit prime numbers		5.2E+72
Electrons in the universe		8.37E+77

Числа на Мерсене (38)

- PGP (Pretty Good Privacy)
  криптиране на файл
  подпис на файл
  имплементации (www.pgp.com, www.pgpi.org, www.gnupg.org)

- PEM (SSL)
  OpenPGP
  CA PKI

- Криптоалгоритми с мрежова значимост
  TLS/SSL

3. Identification & Authentification

- Passwords
  stored password files (backup, superusers)
  encrypted password files
  password rules

атаки (replay, dictionary/guessing, brute-force)
PINs + карта (4-8)
two-stage authentification

- One-time passwords
  shared lists of one-time passwords
  updated one-time passwords

- Challenge-response identification
  Challenge
    random numbers
    sequence numbers
    timestamps

  Challenge-response чрез симетрични алгоритми
    CR чрез симетрично криптиране (Kerberos)
      a) A -> B : Ek(Ta)
      b) A <- B : Rb
         A -> B : Ek(Rb)
      c) A <- B : Rb
         A -> B : Ek(Ra,Rb)
         A <- B : Ek(Rb,Ra)
    CR чрез one-way функции
    hand-held passcode generators

  Challenge-response чрез асиметрични алгоритми
    CR базирани на криптиране
      A <- B : h(r), B, Pa(r,B)
      A -> B : r

    CR базирани на електронен подпис
      a) A -> B : CERTa, Ta, B, Sa(Ta,B)
      b) A <- B : Rb
         A -> B : CERTa, Ra, B, Sa(Ra,Rb,B)
         A <- B : CERTb, A, Sb(Rb,Ra,A)

4. Литература

Diffie, W., and Hellman, M. New directions in cryptography.
Knuth, D.E. The Art of Computer Programming, Vol 2: Seminumerical Algorithms
Rivest, R.L., Shamir, A., Adleman, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems
Schneier, B. Applied Cryptography
Biham, E., Shamir, A. Differential Cryptanalysis of the Data Encryption Standard
Riesel, H. Prime Numbers and Computer Methods for Factorization
Lai, X. On the Design and Security of Block Ciphers
Kahn, D. The Codebreakers
Bamford, J. The Puzzle Palace
Stoll, C. The Cuckoo's Egg