

Roskilde Universitetscenter, Datalogisk Afdeling
E-mail: ncjuul@acm.org



Kryptering

Niels Christian Juul

N&P 11: 2001 April 18th

Om kryptering, DES, RSA, PGP og SSL

© Copyright 1998-2001, Niels Christian Juul

OH-11 DK

1

Kryptografering



- ◆ “encipherment” , “encryption”
- ◆ et spørgsmål om sikkerhed:
 - mod aflytning
 - mod forvanskning eller sletning
 - om hvem afsenderen er
 - for ægthed af “elektronisk underskrift”
- ◆ I alle ISO modellens lag, specielt:
 - 1: fysiske lag (indkodning af signaler)
 - 4: transportlaget (trafikkontrol)
 - 6: repræsentationslaget (datarepræsentation)

© Copyright 1998-2001, Niels Christian Juul

OH-11 DK

2

Elementer i kryptografering



- ◆ Klar tekst (plain text)
- ◆ Krypteringsfunktion (encryption method)
- ◆ Krypteringsnøgle (encryption key)
- ◆ Krypteret tekst (cipher text, cryptogram)
- ◆ Plus den omvendte funktion/nøgle

Det forudsætter at begge ender kender deres

- ◆ funktion
- ◆ nøgle

© Copyright 1998-2001, Niels Christian Juul OH-11 DK

3

Gætteværk



- ◆ Analyse af krypteret tekst m.h.p.
 - sammenligning med klar tekst
 - genkendelse af sekvenser
 - hyppighed af sekvenser
 - kendskab til indhold
- ◆ Arbejdsindsatsen afhænger af udbyttet, fx:
 - en krypteret tekst, der indeholder blivende oplysninger af stor værdi
 - en krypteret tekst, der indeholder oplysninger af mindre værdi og som hurtigt forældes

© Copyright 1998-2001, Niels Christian Juul OH-11 DK

4

Kodebryderens værktøj



- ◆ Opsnappet krypteret tekst
 - jo mere/længere tekst - jo bedre
- ◆ Tid
- ◆ Datamaskiner
 - Analyse af data for frekvens statistik
 - Brute force - gennemsøgning af udfaldsrummet
- ◆ Evt. også
 - kendskab til indholdets emne eller struktur
 - kendskab til krypteringsalgoritme
 - kendskab til nøgle

© Copyright 1998-2001, Niels Christian Juul OH-11 DK

5

Basale krypteringsteknikker



Simple krypteringsmetoder indeholder:

- ◆ rotering af bit-sekvens
 - **transpositioner** (permutationer)
- ◆ XOR af bit med nøgle
 - **substitutioner**
- ◆ ombytning af sekvenser
 - **transpositioner** (permutationer)
- ◆ P-box --- permutering
- ◆ S-box --- substituering

© Copyright 1998-2001, Niels Christian Juul OH-11 DK

6

DES



- ◆ Data Encryption Standard
- ◆ National Bureau of Standards, USA 1977
- ◆ Udviklet af IBM
- ◆ Baseret på et:
 - “product cipher”
- ◆ bestående af en serie af
 - P-box og S-box
- ◆ Tilgængelig som “hardware” siden 1984

© Copyright 1998-2001, Niels Christian Juul OH-11 DK

7

DES komponenter



- ◆ 64 bit klar tekst
- ◆ 56 bit nøgle
- ◆ 19 trin, hvoraf de midterste 16 trin er baseret på:
 - ombytning af to 32 bit grupper
 - en omformning af den ene gruppe ved XOR af denne med en funktion af den oprindelige 32-bit gruppe og trinets nøgle
 - trinets nøgle udregnes også ved ombytninger

© Copyright 1998-2001, Niels Christian Juul OH-11 DK

8

Variationer



- ◆ **DES kan gøres stærkere ved først at fortynde budskabet i klar tekst form**
 - f.eks. indsætte budskabet i en betydningsløs tekst som hvert 7. bogstav
 - eller indsætte betydningsløse tekster i pauser mellem klar tekst
- ◆ **Fordel:**
 - sværere at genkende budskabet efter dekryptering
- ◆ **Ulempe:**
 - spild af tid til kryptering og transmission af betydningsløse data

© Copyright 1998-2001, Niels Christian Juul OH-11 DK

9



- ◆ **Blok kryptering (“block cipher”)**
 - kræver blokke af 64 bit af gangen
 - kryptering og dekryptering indeholder de samme (omvendte) trin, men i modsat rækkefølge
- ◆ **Flydende kryptering (“stream cipher”)**
 - kræver kun et tegn (byte) af gangen
 - hvert nyt krypteret tegn er en funktion af hele den foregående tekst hvilket modvirker frekvensanalyser

© Copyright 1998-2001, Niels Christian Juul OH-11 DK

10

Problemer med DES ?



- ◆ 56 bit nøgle skulle have været 128
- ◆ NSA (USA) krævede den nedsat
- ◆ Ingen begrundelse for trinenes konstruktion offentliggjort
- ◆ Krypteringschip i alle telefoner umuliggør aflytning, selv med dommerkendelse
- ◆ Udveksling af nøgler må gøres af anden vej:
 - så den ikke aflyttes eller omformes
 - så de to “ender” kan tro på hinanden

© Copyright 1998-2001, Niels Christian Juul OH-11 DK

11

Uddeling af nøgle



- ◆ Send et meget stort antal nøgler som hver er gemt i et stort puslespil sammen med deres nummer
- ◆ Nøglemodtageren vælger at løse et puslespil, tager sin nøgle og returnere dens nummer
- ◆ Nu kan uddeleren finde nøglen ud fra nummeret fordi “han” har puslespillene i deres oprindelige (samlede) form.

© Copyright 1998-2001, Niels Christian Juul OH-11 DK

12

Kryptering med nøglepar



- ◆ En besked, P krypteres med krypteringsmetoden E og kan herefter kun dekrypteres med metoden D
- ◆ Tre krav til to-nøglekryptering:
 - $D(E(P)) = P$
 - D kan ikke udledes ud fra kendskab til E
 - E kan ikke brydes selv om man kan prøve sig frem med kendte par P, E(P)

© Copyright 1998-2001, Niels Christian Juul OH-11 DK

13

Public Key Encryption



- ◆ Hver person, f.eks. A og B udstyres med to nøgler istedet for en:
 - en offentlig nøgle, som alle kender, O(A) og O(B)
 - en privat nøgle, som kun personen kender, P(A) og P(B)
- ◆ For at sende en besked, P fra A til B anvendes den offentlige nøgle, O(B) til at bestemme krypteringsmetoden, $E(x) = f(E, O(B), x)$ og sende E(P)

© Copyright 1998-2001, Niels Christian Juul OH-11 DK

14



- ◆ For at kunne genfinde $P = D(E(P))$ skal man kende det til E hørende D, som for B's vedkommende er bestemt af $P(B)$:
- ◆ $D(x) = f(D, P(B), x)$
- ◆ Når blot E og D er parametriseret af det tilhørende nøglepar, kan E og D i sig selv godt være kendte for alle

RSA algoritmen (MIT)



- ◆ Rivest, Shamir og Adleman, 1978
- ◆ Baseret på talteori bl.a. umuligheden af generel primtalsfaktoriserings
- ◆ Først udregnes parametrene:
 - Vælg to meget store primtal, p og q
 - Udregn $n = p \cdot q$ og $z = (p-1) \cdot (q-1)$
 - Vælg d, så d og z ikke har fælles primfaktorer
 - Bestem e, så $e \cdot d = 1$ modulo z

RSA



- ◆ Klar tekst i klumper af P bestående af mindre end n bits
- ◆ krypteres til $C=E(P)$, hvor:
 - $E(P) = P^e \pmod{n}$
- ◆ og dekrypteres tilbage igen til $P=D(C)$:
 - $D(C) = C^d \pmod{n}$
- ◆ således er de to nøgler:
 - (e, n)
 - (d, n)

© Copyright 1998-2001, Niels Christian Juul

OH-11 DK

17

RSA mærkværdigheder



- ◆ RSA betragtes som **ammunition/våben** i USA
- ◆ RSA er **patenteret** og sælges kommercielt indenfor USA
- ◆ RSA må **ikke eksporteres** og er derfor heller ikke patenteret udenfor USA
- ◆ RSA-lignende algoritmer kan derfor **frit bruges udenfor USA** bare ikke de tages over grænsen
- ◆ Endvidere må de **krypterede beskeder** godt **krydse grænsen**

© Copyright 1998-2001, Niels Christian Juul

OH-11 DK

18

Digitale signature



- ◆ Identiteten på afsenderen fastlægges
 - for at overbevise modtageren
 - for at afsenderen ikke senere kan nægte
- ◆ P.g. af aflytning m.v. er det ikke nok at identificere sig med brugernavn og løsen ved opkobling til modtageren
- ◆ Public Key Encryption løser imidlertid problemet

© Copyright 1998-2001, Niels Christian Juul OH-11 DK

19

Sikkerhed på Internettet



- ◆ Eftersom det underliggende lag 3 net (IP) befordrer vores data over forbindelser og maskiner, som andre bestemmer over, kan vi ikke vide os sikre mod aflytning af vores data.
- ◆ Den totale mængde af data på Internettet gør det dog ikke så sandsynligt.
- ◆ To eksempler på sikkerhedsudvidelser:
- ◆ **PGP - Pretty Good Privacy**
 - skaffer sikkerhed for e-mail
- ◆ **SSL - Secure Socket Layer**
 - skaffer sikker kanal for WWW (http)

© Copyright 1998-2001, Niels Christian Juul OH-11 DK

20

PGP - Pretty Good Privacy



- ◆ Et “public key encryption” system med en offentlig og en privat nøgle til hver
- ◆ Mulighed for forseglede breve
- ◆ Mulighed for digitale signature
- ◆ Mulighed for flere modtagere af samme brev

© Copyright 1998-2001, Niels Christian Juul OH-11 DK

21

PGP Problemer



- ◆ Hvem giver mig den offentlige nøgle på den anden part i en kommunikation ?
- ◆ Kan andre underskrive i mit navn ?
- ◆ Hvordan sikre jeg mig mod “lokal” aflytning før beskeden krypteres ?

© Copyright 1998-2001, Niels Christian Juul OH-11 DK

22

SSL - Secure Socket Layer



- ◆ World Wide Web kommercielt på vej
- ◆ Ønsker om overførsel af fortrolige oplysninger fra “client” til “server”
- ◆ Ønsker om pengeoverførsler
- ◆ SSL indlægges som et lag mellem TCP/IP og HTTP
- ◆ Kræver at man har oprettet sin identitet hos en nøgleudsteder
- ◆ **Netscape**

© Copyright 1998-2001, Niels Christian Juul OH-11 DK

23