Koder og kryptering

Foredrag UNF

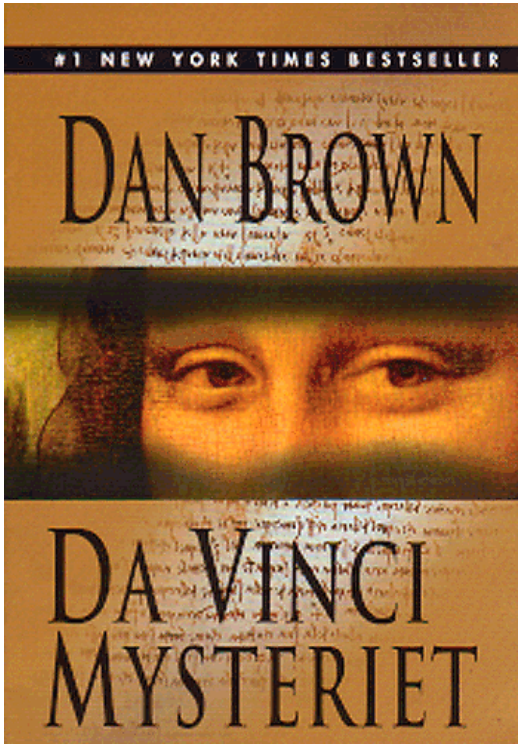
4. december 2009

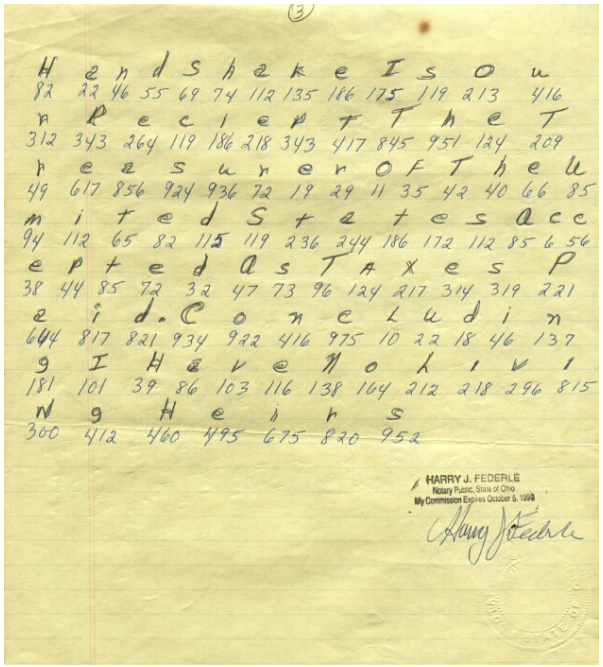
Erik Zenner

(Adjunkt, DTU)

I. Indledende bemærkninger

Hvad tænker I på, når I hører ”kryptologi”?





Hvad tænker jeg på, når jeg siger ”kryptologi”?

- Den matematiske del af kommunikationssikkerheden.
- Mange flere mål end kun ”fortrolighed”. F.eks.:
  - Fortrolighed
  - Autenticitet
  - Integritet
  - Uafviselighed
  - Identifikation
  - Anonymitet
  - …

Planen for i dag

- Overblik over kryptologiens mange aspekter
  - Kryptologiens historie
  - Den kryptologiske værktøjskasse
  - Den mørke side
- Nødvendigvis kun få detaljer

II. Lidt historie

II.1 Klassiske chifre

Substitutionschiffer (1)

- Det mest kendte chiffer overhovedet:
  - Mere end 2000 år gammel!
- Hvordan fungerer det?
  - Opdel klarteksten i symboler (f.eks. bogstaver)
  - Erstat (”substituer”) hvert symbol med et andet (f.eks. et andet bogstav, et tal, et mystisk symbol)
- Eksempel:
  - ♎♏♦ ♒♏❒ ♏❒ ♏■ ❍♏■♓■♑⬧●□♏⬧ ♎♋■⬧& ♦♏&⬧♦ ♒❖□❒ ♌□♑⬧♦♋❖♏❒■♏ ♌●♏❖ ♏❒⬧♦♋♦♦♏♦ ❍♏♎ ⬧♓■♑♎♓■♑⬧🕭⬧🖂❍♌□●♏❒

Substitutionschiffer (2)

- Hvordan analyserer man et substitutionschiffer?
- Vi starter med at betragte de hyppigste symboler:
  - ♏ (14x), ♦ (8x), ⧫ (8x), ■ (7x), ❒ (6x)
- Vi formoder, at de svarer til de hyppigste danske bogstaver (E, S, T, N, R):
  - ♎ET ♒ER ER EN ❍EN♓N♑S●□ES ♎♋NS& TE&S⧫ ♒❖□R ♌□♑ST♋❖ERNE ♌●E❖ ERST♋TTET ❍E♎ ♦♓N♑♎♓N♑S🖃 S♈❍♌□●ER
- Vi kan nu gradvist erstatte symboler med bogstaver indtil vi når frem til den rigtige løsning.

Substitutionschiffer (3)

- I almindelighed:
  - Det samme symbol bliver altid krypteret på samme måde
  - Hyppigheden i klarteksten = hyppighed i chifferteksten
  - Substitutionschiffer kan knækkes hvis angriberen har tilstrækkelig mange krypterede symboler til rådighed
- Substitutionschifre er spændende for gåder (og bøger som "Da Vinci Mysteriet"), men ikke sikker i praksis.

Transpositionschiffer (1)

- Endnu ældre chiffer:
  - Allerede kendt for 2500 år siden!
- Hvordan fungerer det?
  - Opdel klarteksten i symboler (f.eks. bogstaver)
  - Lav om på bogstavernes rækkenfølge
- Eksempel:
  - dtbktjaaeelrvafbnkeeeeeensvvdlnletsehpt

Transpositionschiffer (2)

- Hvordan analyserer man et transpositionschiffer?
- Afprøv forskellige transpositioner, f.eks. ved at læse hver i-te bogstav i teksten (som i nedenstående tabel):

D	E	N	N	E
T	E	K	S	T
B	L	E	V	S
K	R	E	V	E
T	V	E	D	H
J	A	E	L	P
A	F	E	N	T
A	B	E	L	

- Analysemetoder for mere indviklede transpositionschifre findes også $\Rightarrow$ heller ikke sikker i praksis!

II.2 Maskinernes tidsalder

Kerckhoffs' princip

- Spørgsmål:
  - Hvorfor gik vi egentlig ud fra, at angriberen kender algoritmen?
- Svar:
  - I praksis kan han typisk finde ud af den!
- Kerckhoffs princip (1883):
  - Sikkerheden af en krypteringsløsning må ikke afhænge af algoritmens, men kun af nøglens hemmelighed.
- Hvis angriberen finder ud af krypteringsmetoden:
  - Med Kerckhoffs' princip: Bare brug ny nøgle
  - Uden Kerckhoffs' princip: Brug et helt nyt chiffer

En ny udvikling

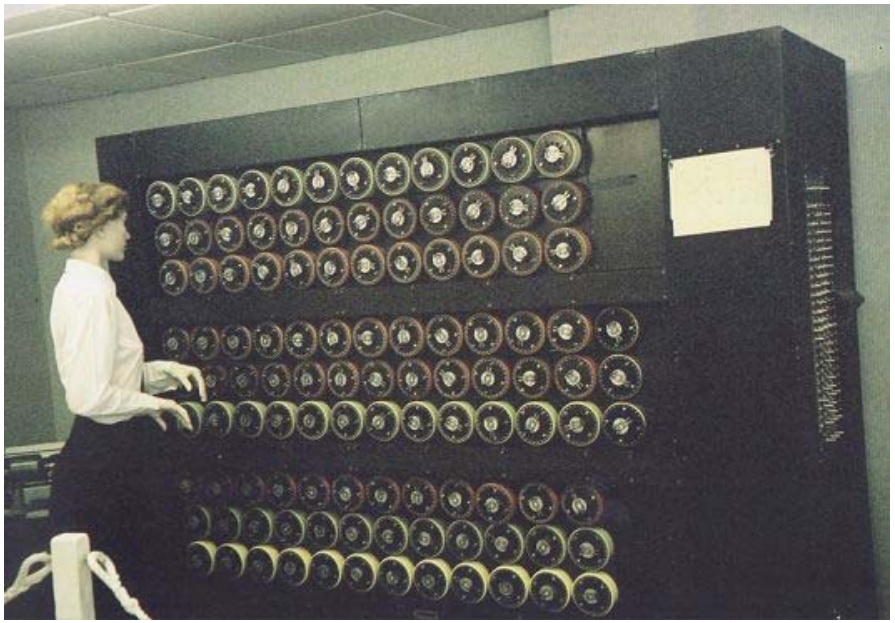
- Under 1. verdenskrig:
  - Rigtig mange af de gamle chifre blev knækkede
  - Behov for bedre kryptering
- Problem:
  - Mennesker er ikke gode til at kryptere i hånden
  - Bedre løsninger kan udvikles, men ikke bruges
- Løsning:
  - Udvikling af krypteringsmaskiner

Rotormaskiner

- Berømt eksempel: Enigma
- Klartekst stadigvæk opdelt i bogstaver, men:
  - Transpositionschiffer
  - Flere substitioner
  - Transpositionschiffer
- Derudover ændrer substitutionerne sig med tiden (rotorer)!

Computerens opfindelse

- Tyskerne var overbevist om, at Enigmaen ikke kan knækkes.
- Men:
  - Kryptoanalytikerne fandt nogle svagheder
  - Matematikerne opfandt computeren!
  - Mange flere nøgler end forventet kunne testes!
- Igennem 2. verdenskrigs sidste år var Enigmaen *de facto* knækket!



II.3 Nutidens kryptologi

Store forandringer

- Inden 1970:
  - Kryptologi som privilegium for diplomater, efterretningstjenester og militær.
- I 1970erne:
  - Kommunikationssamfund begynder for alvor at udvikle sig; computere spreder sig, opfindelse af Internettet.
  - Bankerne kræver kryptologisk beskyttelse af deres kommunikation.
  - Den første offentlige krypteringsstandard (DES) i 1976.
  - Opfindelse af public-key kryptering i 1976.
  - Interessant område for matematikere, offentlig forskning udvikler sig.

Status i dag

- Kryptologi er ikke længere en militær, men en civil disciplin.
- Stor offentlig forskning indenfor emnet.
- Kryptologi gammerer sig bag mange anvendelser, som f.eks.
  - Betalings- og adgangskort
  - Internetsikkerhed
  - Mobiltelefoner
  - Bilnøgler
  - Trådløs kommunikation
  - Tyverisikring
  - …

III. Den kryptologiske værktøjskasse

III.1 Secret-key kryptologi

Secret-key kryptologi

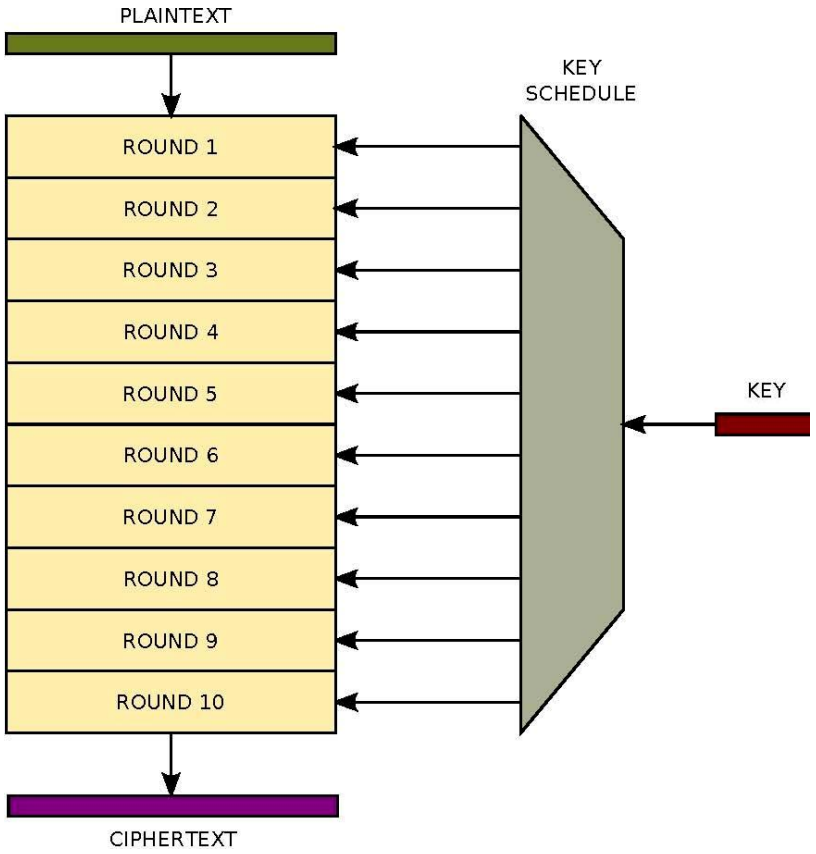
- Klassisk model:
  - Algoritmen er offentlig
  - Afsender og modtager deler en hemmelig nøgle
- Mest udbredte opgaver:
  - Fortrolighed (kan beskeden læses af andre?)
  - Autenticitet (stammer beskeden fra afsenderen?)
  - Integritet (er beskeden uændret?)
- Lad os kort kigge på hvordan man løser fortrolighedsproblemet i dag…

Historie: AES

- Data Encryption Standard (DES) fra 1976 var ved at blive gammel
- 1997: Amerikansk NIST starter offentlig konkurrence om ny krypteringsstandard
- 1998: 15 nye chifre bliver forslået
- 1998-2000: Offentlig analyse af kandidaterne
- 2000: Vinderen ”Rijndael” bliver kåret som den nye ”Advanced Encryption Standard” (AES)
- 2009: Første revner viser sig i AES…

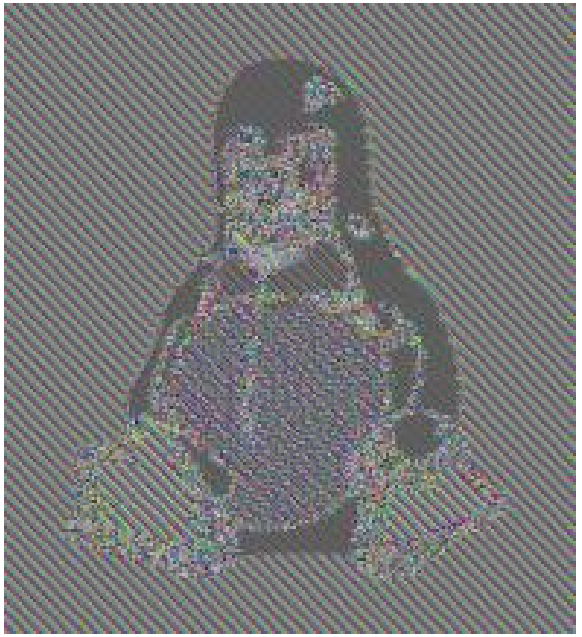
Blokchiffer

- AES er et såkaldt blokchiffer:
  - Tager en inputblok (128 bit)
  - Kører krypteringsalgoritme under kontrol af en nøgle
  - Leverer outputblok (128 bit)
- Hver runde består af:
  - Et substitutionschiffer
  - Et transpositionschiffer



Blokchiffer = Substitionschiffer

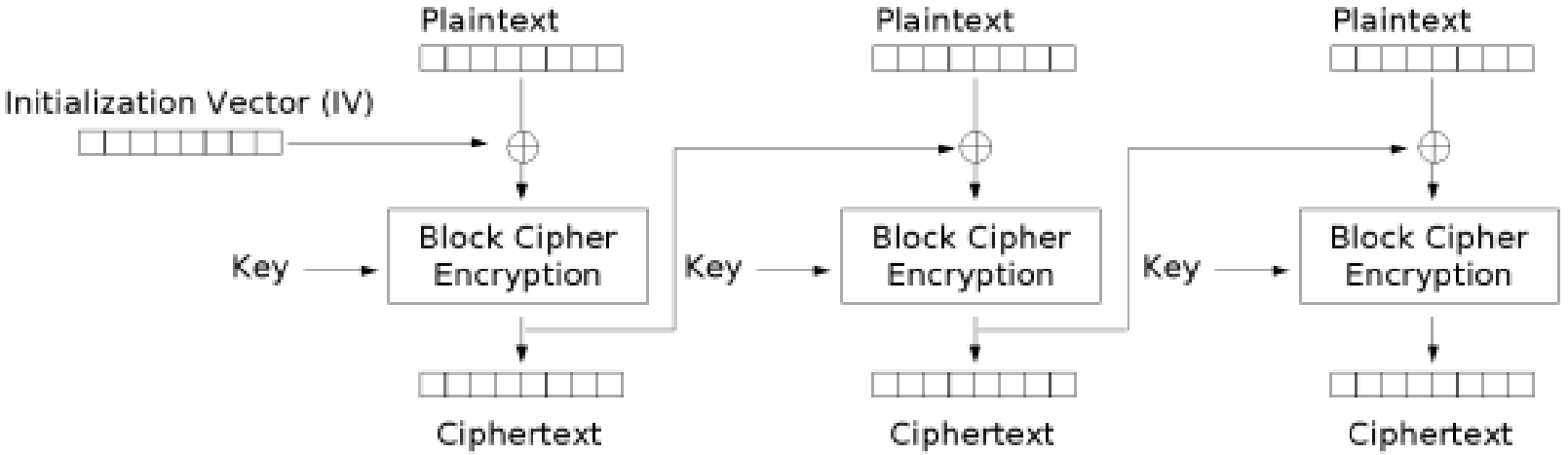
- Vi ved:
  - Et substitutionschiffer deler beskeden op i blokke
  - Hver blok krypteres på samme måde
- Med andre ord:
  - AES er et substitutionschiffer
  - Substitutionschifre er usikre!
- Vi mangler ”rotorprincippet”!



Original image by Larry Ewing, lewing@isc.tamu.edu, using GIMP

Modes of operation

- I virkeligheden bruger vi AES og andre blokchifre vha. en såkaldt mode of operation:
  - IV sikrer at lige beskeder bliver krypteret på forskellig vis
  - Runder sikrer at lige blokke bliver krypteret på forskellig vis

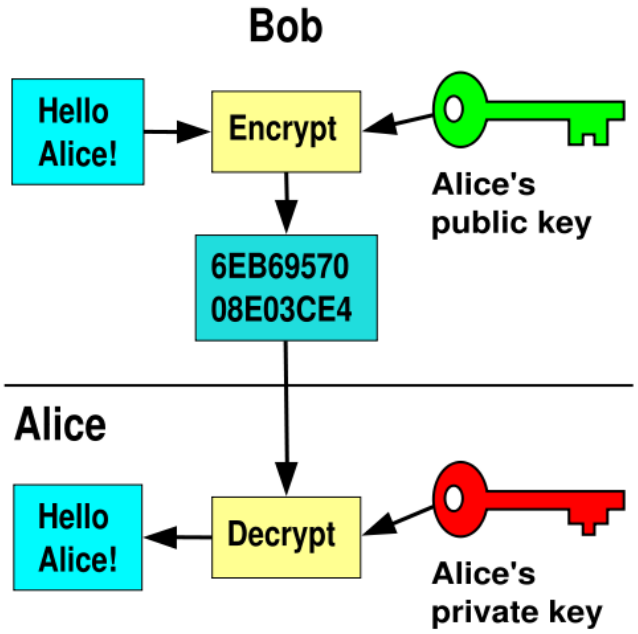


Cipher Block Chaining (CBC) mode encryption

III.2 Public-key kryptologi

Public-Key kryptologi

- Problem med secret-key kryptologi:
  - Nøgleudveksling
  - Eksempel: At handle på Internettet
- Idé public-key kryptologi:
  - Brug forskellige nøgler til kryptering og dekryptering!
  - Offentlig nøgle til kryptering:
    - Findes i en telefonbog
    - Alle kan sende beskeder til Alice
  - Privat nøgle til dekryptering:
    - Hemmelig!
    - Kun modtageren kan dekryptere



Det store spørgsmål

- Public-key idé:
  - Diffie / Hellman, 1976
  - Merkle, 1974 (?)
  - Ellis, 1969 (?)
- Men kan det overhovedet lade sig gøre?
  - Intuition 1: Brevkasse
  - Intuition 2: Shamirs No-Key protokol (se tavle)
  - Intuition 3: Diffie-Hellman systemet
- I praksis kender angriberen den offentlige nøgle:
  - Kan han så ikke beregne den private nøgle?
  - Kan han så ikke kryptere alle sandsynlige beskeder og sammenligne med chifferteksten?

RSA systemet (1)

- Rivest / Shamir / Adleman 1978:
  - præsenterer en matematisk løsning
  - bruger et vanskeligt problem fra talteori
- Faktoriseringsproblemet:
  - Lad p, q være to store primtal (> 500 bit), og lad $N = p \cdot q$.
  - Hvis man kun kender N, så er det vanskeligt at finde p og q.

RSA systemet (2)

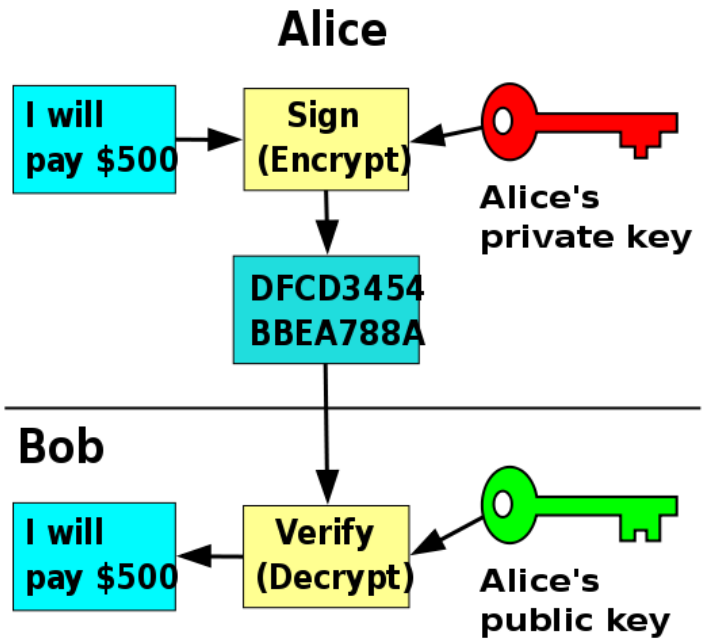
- Forberedelse:
  - Modtageren vælger primtal p og q og beregner $N = p \cdot q$.
  - Han vælger også et "passende" heltal e.
  - Han gør N og e offentligt og holder p og q hemmeligt.
- Det er let at kryptere en besked ved at beregne

$$y = x^e \bmod N,$$

  hvor "mod N" er resten når man dividerer med N.
- Det er svært at dekryptere y, medmindre man kender p og q.
- Flere detaljer: Forelæsninger eller bøger om kryptologi.

Digital signatur

- Vi kan også vende public-key kryptering på hovedet for at få digitale signaturer:
  - For at skrive under på en besked "dekrypterer" jeg den vha. min private nøgle. Husk at kun jeg kan gøre det!
  - For at verificere signaturen krypterer modtageren den og tjekker om den nu giver mening. Husk at alle kan gøre det!
- Resultat: Uafviselighed!



III.3 Fantastiske protokoller

Fantastiske protokoller

- Med modern kryptologi kan man også løse mange problemer som umiddelbart virker uløselige, som f.eks.:
  - **Anomymitet:** Kan vi surfe på Internettet eller sende mails uden at en næsten alvidende "Big Brother" kan se hvad vi gør?
  - **Online poker:** Kan vi spille Online-Poker (uden udbyder!) mod hinanden uden at nogen kan snyde de andre?
  - **Zero-knowledge proofs:** Kan jeg bevise, at jeg kender en hemmelighed, uden at røbe hvad den er?
  - **Secret sharing:** Kan vi dele en hemmelighed blandt 5 personer således at enhver sæt af 3 personer kan genskabe den?
  - …


IV. Den mørke side

IV.1 Kryptoanalyse

Den offentlige kryptoanalyses rolle

- Kerckhoffs' princip:
  Sikkerheden må kun afhænge af nøglens hemmelighed, ikke algoritmens hemmelighed.
  - Algoritmen kan lige så godt gøres offentlig
- **Argument:** Men min algoritme bliver vel ikke mindre sikker fordi jeg holder den hemmelig?
- **Modargument:** Hvordan ved du, at din algoritme er sikker, hvis ingen har kigget på den?
  - Algoritmer skal analyseres offentligt

Eksperter inden for kryptoanalyse

- Typ 1: Frie kryptoanalytikere
  - Arbejder typisk for universiteter
    (nogle gange også virksomheder eller selvstændig)
  - Deler deres viden om kryptologi
  - Formål: Forbedring af systemsikkerheden
- Typ 2: Angribere
  - Arbejder typisk for efterretningstjenester
    (nogle gange også virksomheder eller kriminel miljø)
  - Deler ikke deres viden om kryptologi
  - Formål: Knække og udnytte systemet

Derfor:

- Udnyt de frie kryptoanalytikers viden
- Tiltro til kryptologiske løsninger opnås ved offentlig analyse som ikke finder svagheder!
  - Offentlige beskrivelser / standarder
  - Offentlige implementeringer (Open Source)
- Restrisiko: Angriberne deler ikke deres viden!
  - Angriberne ved alt som de frie kryptoanalytikere ved, men ikke omvendt.
  - Eksempel: DES

Eksempler på teoretiske angreb

- Analyse af DES
  - mange teoretiske resultater, dog ingen praktiske angreb
  - offentligt projekt (AES) for at finde efterfølger
- Analyse af RC4
  - finder flere og flere dårlige egenskaber
  - offentligt projekt (eStream) for at finde potentiel efterfølger
- Analyse af MD5, SHA-0, SHA-1 (f.eks. i HTTPS):
  - er knækkede
  - offentligt projekt (SHA-3) for at finde efterfølger
- Analyse af AES
- …

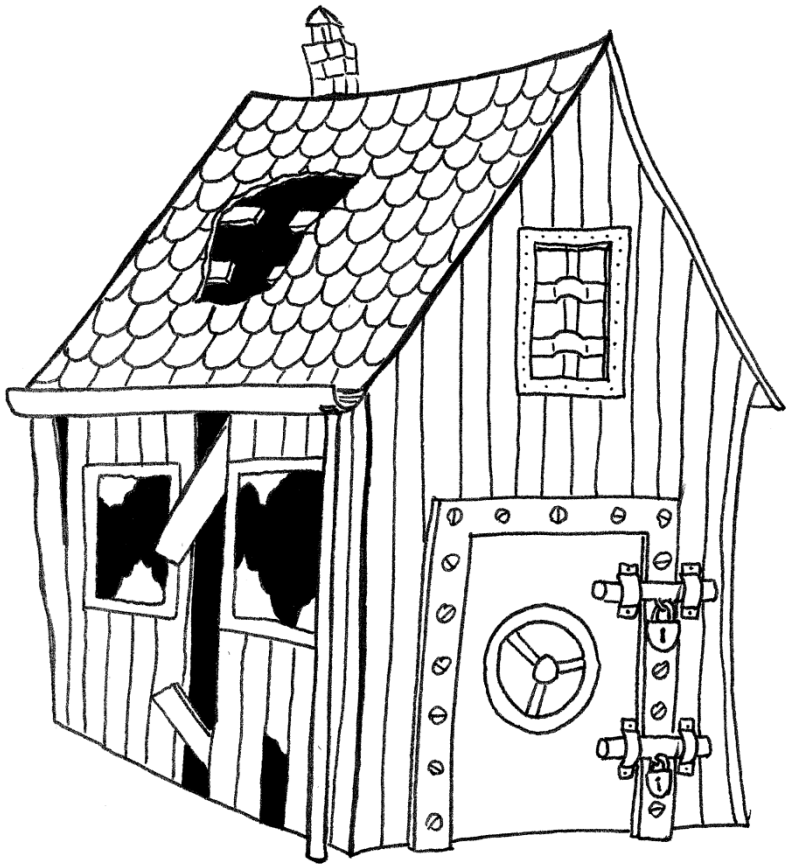
Eksempler på praktiske angreb

- Netscape (1996)
- GSM mobiltelefoner (1997)
- PGP (2000)
- Bluetooth (2001)
- WEP (2001)
- Microsoft Word (2005)
- SpeedPass (2005)
- Debian OpenSSL (2008)
- Mifare classic (2008)
- ….

IV.2 Om papvægge og ståldøre

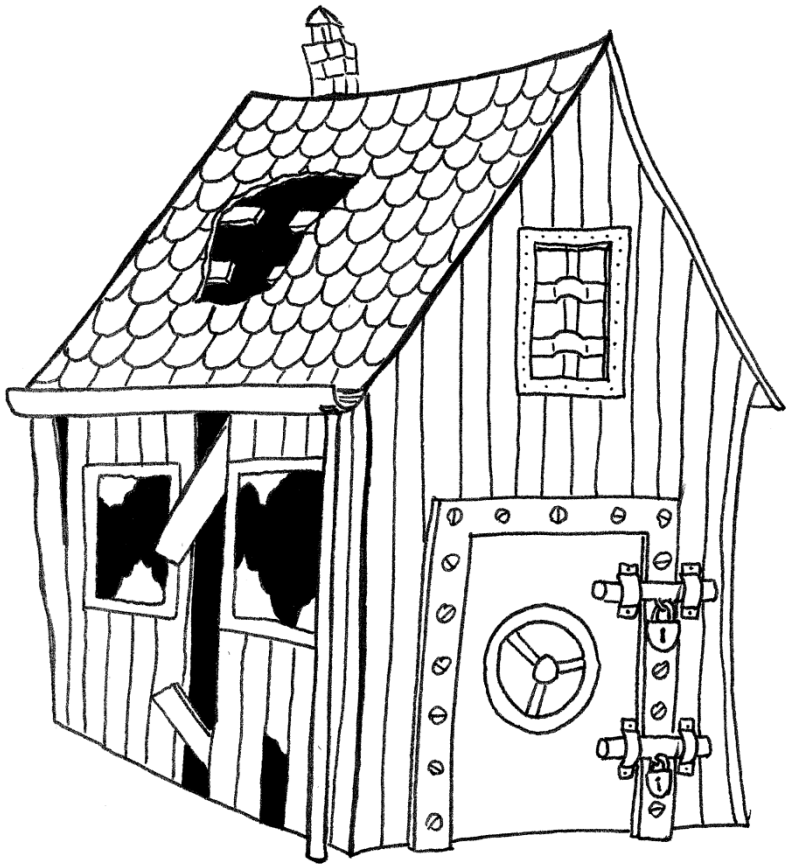
”Det svageste led”-princippet

- Mange formoder at de frie kryptoanalytikere er ca. på højde med angriberne.
- Hypotese: De fleste kryptologiske standarder i dag er sikre.
- Men det er ikke ensbetydende med, at sikkerhedsløsningen er sikker.
- Tænk på kryptologi som en byggeklods i den samlede sikkerhedsarkitektur.



”Det svageste led”-princippet

- Angriberen går altid efter det nemmeste mål.
- Hvis kryptologi er for stærk, angrib andre komponenter:
  - Hacking
  - Virer, Trojanere,…
  - Social Engineering
  - Tyveri, indbrud, bestikkelse, afpresning, trudsler, vold…



IV.3 Kryptologi som trudsel

Sikker kommunikation for alle?

- Selvfølgelig kan alle beskytte deres kommunikation vha. kryptologi:
  - også terrorister, bander, rockere, pædofile,…
- Politisk diskussion:
  - Skal kryptologi forbydes (f.eks. USA)?
  - Skal kryptologi begrænses (f.eks. Storbritannien)?
  - Skal regeringen få særlige værktøjer mod kryptologi (f.eks. Tyskland)?
  - Skal kryptologi være fri for alle?
- Problem:
  - Følger kriminelle de love der forbyder kryptologi?
  - Steganografi kan bruges for at dække over brug af kryptologi

Nyt om hacking og kryptologi

- Ransomware:
  - Virus krypterer harddisken og kræver ”løsepenge”
  - Før: Kryptologi er ”passiv”.
  - Nu: Kryptologi som aktivt hackervåben
- Botnets:
  - Hackeren installerer virus på mange computere.
  - Bruger computerne til at knække krypteringsalgoritmer.
  - Giver hackeren regnekraft på linje med efterretningstjenester!

V. Afsluttende bemærkninger

Blik tilbage: Lidt af hvert

- Lidt om kryptologiens historie:
  - Substitutions- og transpositionschifre
  - Rotormaskiner og computere
  - Kryptologi i dag
- Lidt om den kryptologiske værktøjskasse:
  - Blokchifre, AES, mode of operation
  - Public-key kryptologi, RSA, digital signatur
  - Fantastiske protokoller
- Lidt om den mørke side:
  - Kryptoanalyse
  - Angreb i den virkelige verden
  - Kryptologi som trudsel

Hvor kan jeg lære mere?

- Bøger om kryptologi:
  - Simon Singh: Kodebogen (historisk)
  - Niels Ferguson, Bruce Schneier: Practical Cryptography (teknisk)
  - Douglas Stinson: Cryptography (matematisk)
  - *og mange flere*
- Forelæsninger om kryptologi på DTU:
  - DTU har mange forskellige forelæsninger om kryptologi: Krypto 1-3, Anvendt kryptologi, Praktisk Kryptoanalyse,…
  - DTU tilbyder også fremvisning af og introduktion til Enigma (kontakt Matematicum)