Passord, entropi og kryptologi

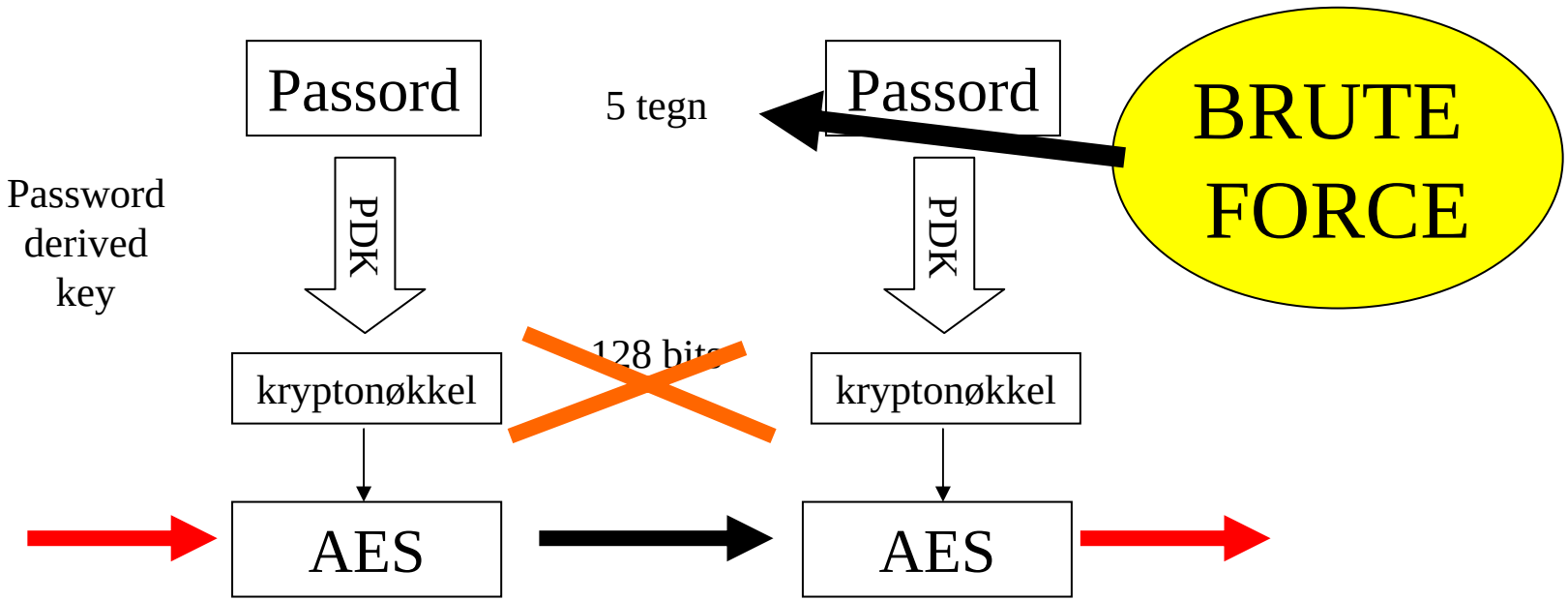
- litt oversikt, noen observasjoner og enkelte anekdoter

NKS'07

Anders Paulshus
Conax AS

Motivasjon

- Passord ofte initiell entropi i kryptografiske anvendelser
- Passord blir da gjerne svakeste ledd (ved uttømmende søk)
- Forståelse av entropi i passord og angrepsmåter viktig



Høyentropipassord er sjelden vare

- Vanlige passord (ca. 10 tegn) er sjelden sterkere en DES

Table 10: Key Size/Password Size Equivalence

Key bits	10 decimal digits	26 letters	36 letters & numbers	94 keyboard characters	1000 word dictionary
56	17	12	11	9	6
64	20	13	13	10	7
80	25	17	16	12	8
112	34	24	22	17	11
128	39	27	25	20	13

- NB: Denne tabellen forutsetter at passordene er generert med uniform distribusjon på alle tegn

Off-line vs. on-line

- Angrep deles ofte inn i ”off-line” og ”on-line”
- ”On-line”: angriperen må følge en bestemt protokoll
  - Eksempel: Minibank PIN
  - Mottiltak: Utestenging, varsling, forsinkelse
- ”Off-line”: angriperen har full frihet til å gjøre uttømmende søk
  - Eksempel: Programvarebasert harddiskkryptering

Angrep:
On-line -> Off-line

- Hvis systemet er bygget for å motstå ”on-line” angrep, kan angriperen vinne mye på komme i en ”off-line” modus.

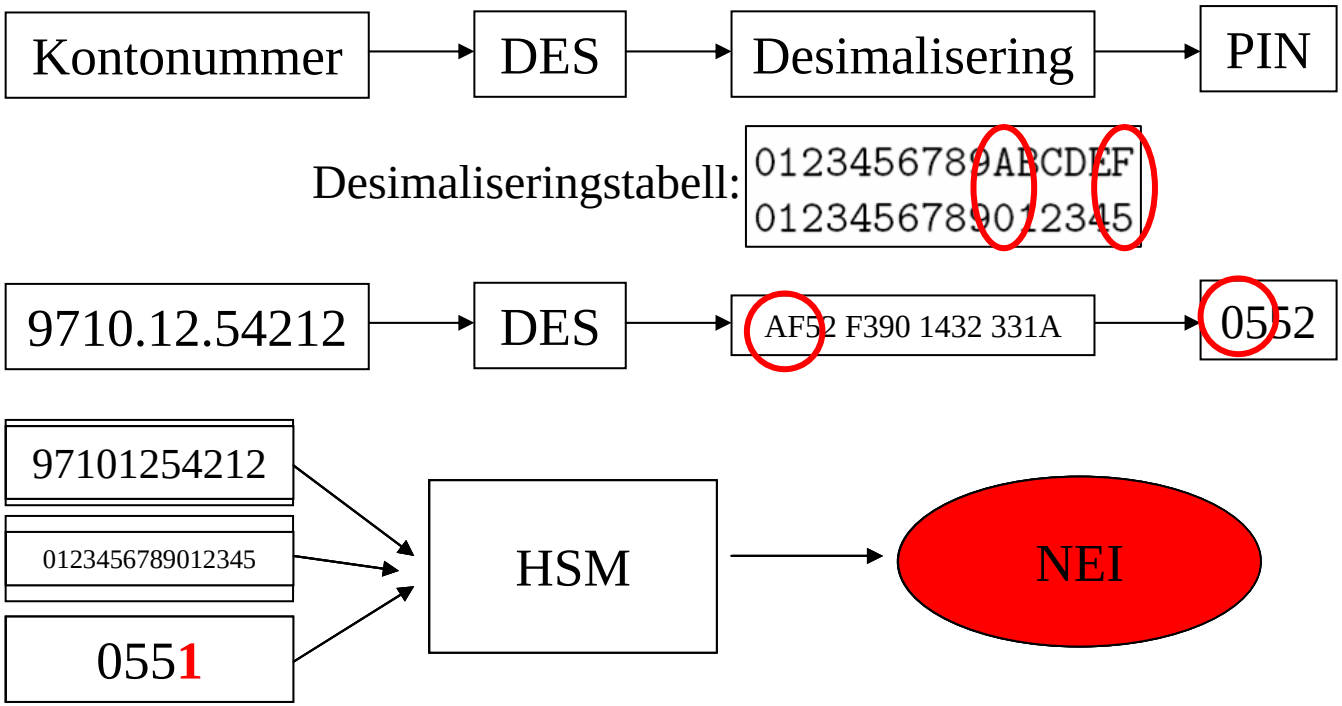
- Eksempel:

  Pålogging til datamaskin (PC/UNIX) gjennom påloggingsvinduet er ”on-line”

  Tilgang til passordhashfilen gjør angrepet til ”off-line”

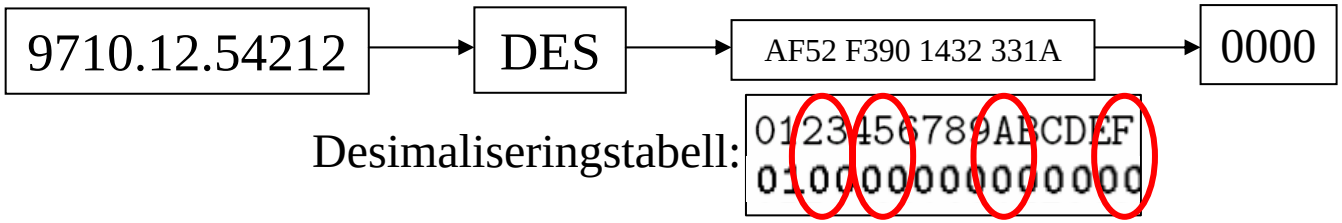
Angrep: Svakheter i protokollen

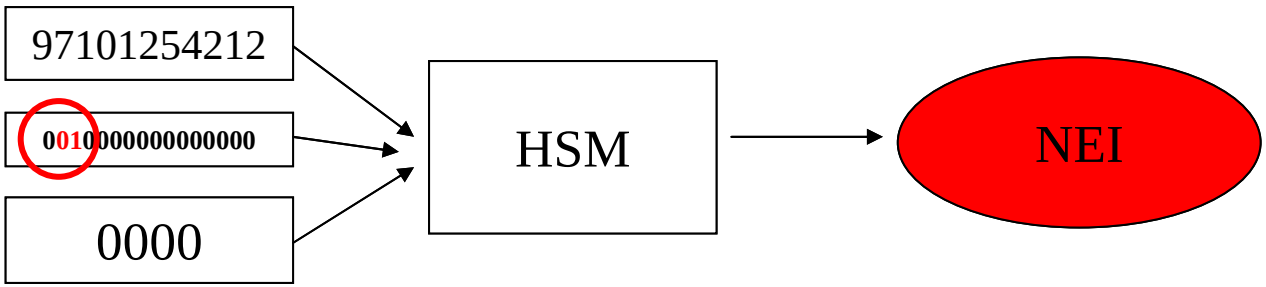
- Eksempel – Minibank-PIN beregning HSM



- Uttømmende PIN-søk: Gj.snitt 5000 forsøk før treff

Desimaliseringstabellen kan endres





Ergo:

PIN inneholder ikke tallet 1

PIN inneholder tallet 2

- Et optimalisert angrep vil i gjennomsnitt kreve 15 forsøk

Angrep: Uttømmende søk på brukernavn

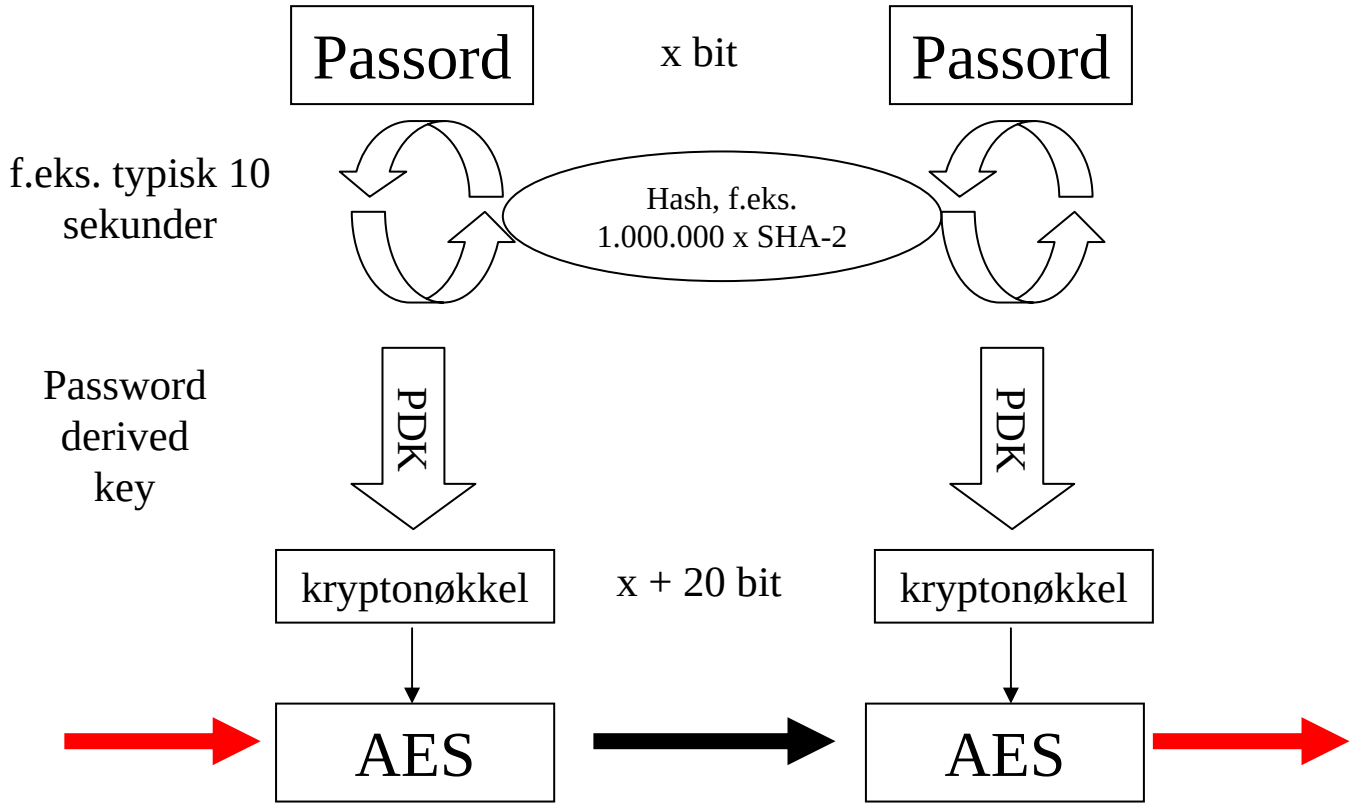
- Protokoll som sperrer uttømmende søk på passord
- Mange (og kanskje veldefinerte) brukere

- -> ”uttømmende søk” på brukernavn.

  Eksempel: Angrep på Skandiabanken som beskrevet av Thomas Tjøstheim

”Off-line” -> ”On-line”

- Kan legge inn en forsinkelse selv ved ”off-line” ved å kreve at passordet skal kvernes ”mye” før det sendes til PDK.



Hvordan sette krav til entropi

- Gjøres gjerne med krav til lengde og kompleksitet
  - Paradoks: Krav til lengde og kompleksitet reduserer entropien

For å gjøre rasjonelle valg må man:

- Gjøre betraktninger om nøkkelrommets størrelse
  - Eksempel: 4 siffer PIN
- Kjenne beskyttelsesmodellen
  - Eksempel: NTLM – gjør alt om til versaler og deler opp passordet i 7 tegns bolker og
- Kjenne angrepsmodellen
  - Eksempel: Ordboksangrep
- Kjenne brukerne
  - Eksempel: Krav til pin >= 7 for å unngå fødselsdato

Optimal ”anti-skimming” PIN

- Mai 2006: Minibankkunder på østlandet svindles vha. påmonterte ”skimmere” og pulver på tastene.
- Pulveret avslører hvilke siffer som inngår i PIN, men ikke rekkefølgen.
- Hvilken PIN-strategi bør velges før å minimere muligheten for at svindelen lykkes?
  - 1 tegn? For eksempel 1111
  - 2 forskjellige tegn? Eks. 1112
  - 3 forskjellige tegn? Eks. 1232
  - 4 forskjellige tegn? Eks. 1234

Antall n-tegns PIN med k ulike tegn

	n = 4	n = 5	n = 6	n = 7	n = 8	n = 9	n = 10
k = 1	1	1	1	1	1	1	1
k = 2	14	30	62	126	254	510	1022
k = 3	36	150	540	1806	5796	18150	55980
k = 4	24	240	1560	8400	40824	186480	818520
k = 5		120	1800	16800	126000	834120	5103000
k = 6			720	15120	191520	1905120	16435440
k = 7				5040	141120	2328480	29635200
k = 8					40320	1451520	30240000
k = 9						362880	16329600
k = 10							3628800

Kodelås med ”løpende forsøk”

- Normalt vil en kodelås vil kreve at hver PIN forsøkes separat.
  - Eks. inntasting 12345678 vil låse opp 2 PIN-koder: 1234 og 5678 men ikke for eksempel 3456.
- 4-sifert pin krever i gjennomsnitt 10.000*4 = 40.000 tastetrykk for garantert å finne PIN
- Enkelte kodelåser godtar ”løpende forsøk”.
  - Eks. inntasting 12345678 vil låse opp 5 PIN-koder: 1234, 2345, 3456, 4567 og 5678.
- Hvor mange tastetrykk kreves for å gjennomløpe alle PIN-koder?
- Kan åpenbart ikke gjøres på mindre enn 10.003 tastetrykk.

Takk for oppmerksomheten

anders . paulshus (at) conax . com

Referanser

- Mike Bond, Piotr Zielinski: Decimalisation table attacks for PIN cracking
- FIPS SPECIAL PUBLICATION 800-57 – Draft January 2003: RECOMMENDATION FOR KEY MANAGEMENT
- Thomas Tjøstheim: A Critical view on Public Key Infrastructures, UiB 2004
- Dwork, Goldberg, Naor: On Memory-bound Functions for Fighting spam, Crypto 2003
- http://forbruker.no/pengenedine/bankogforsikring/article1310127.ece
- http://blogs.msdn.com/si_team/default.aspx