



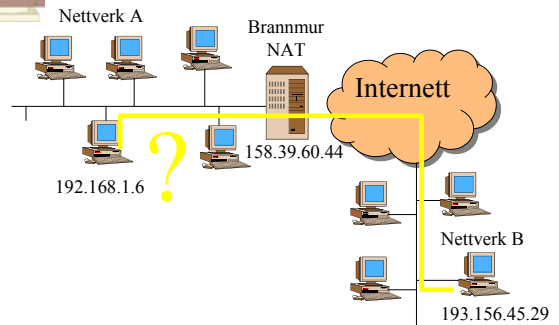
Forelesning 2

Introduksjon til nettverkssikkerhet

11174 Datasikkerhet



Først: En digresjon om IP-telefoni



11174 Datasikkerhet

3. september 2002 Side 2



Tre fundamentet for datasikkerhet

- ▶ **Konfidensialitet**
 - ▶ Kun den som er autorisert har tilgang
- ▶ **Integritet**
 - ▶ Informasjon er ikke endret av uvedkommende
 - ▶ Avsenderen er den den gir seg ut for
- ▶ **Tilgjengelighet**
 - ▶ Informasjon og ressurser er tilgjengelige for autoriserte brukere når disse har behov for det

11174 Datasikkerhet

3. september 2002 Side 3



... som igjen hviler på

- ▶ **Autentisering**
 - ▶ Konfidensialitet/Tilgjengelighet:
Uten autentisering, hvordan kan man avgjøre hvem som har rettmessig tilgang?
 - ▶ Integritet:
(Implisitt) Hvordan kan man avgjøre hva som er den opprinnelige informasjonen?

11174 Datasikkerhet

3. september 2002 Side 4



Grafisk framstilling



11174 Datasikkerhet

3. september 2002 Side 5

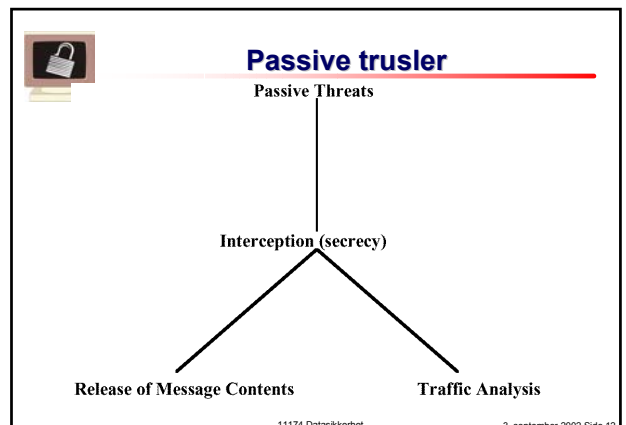
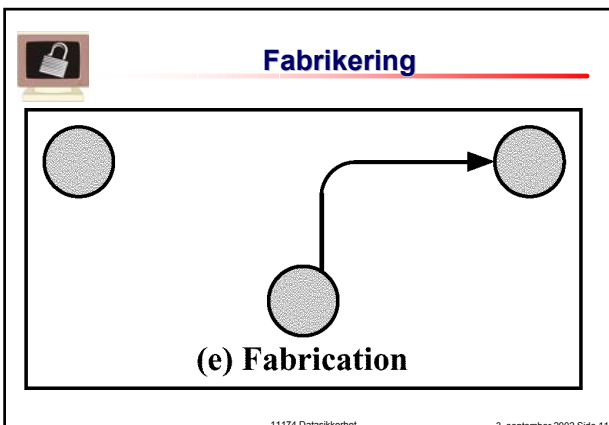
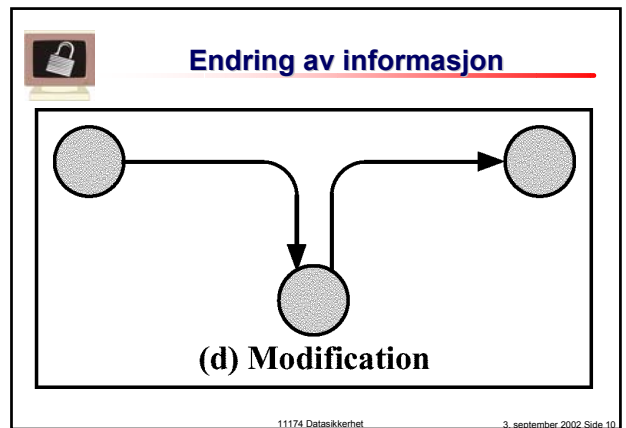
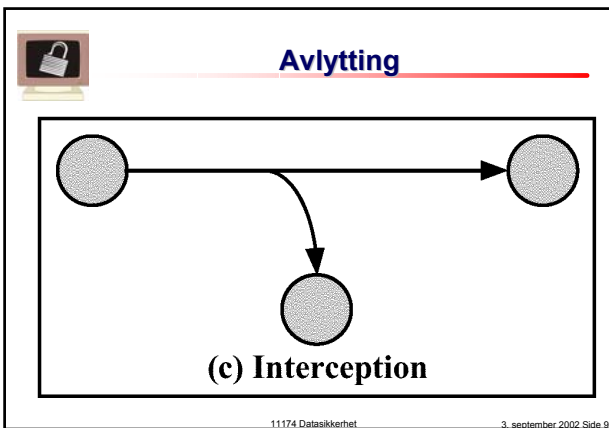
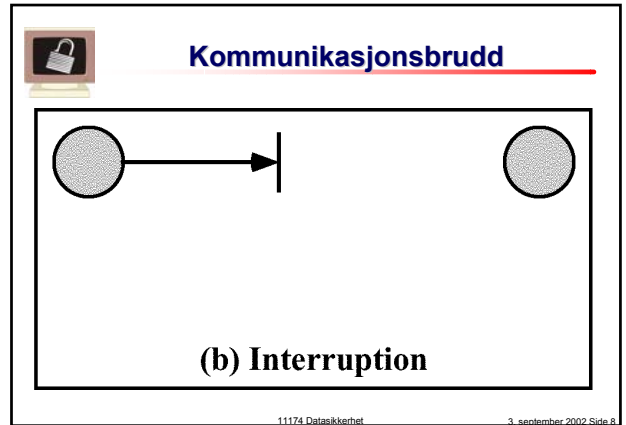
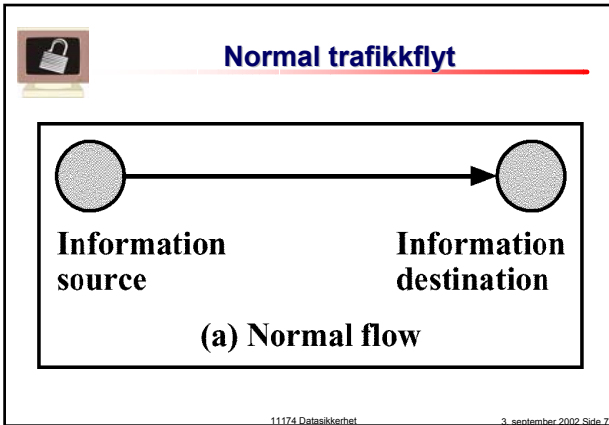


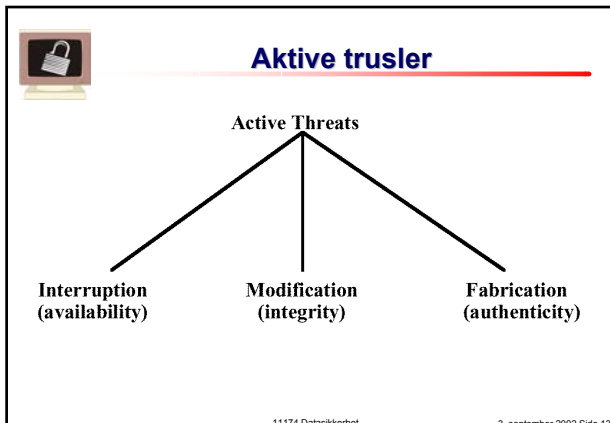
Sikkerhetstrusler

- ▶ Kommunikasjonsbrudd
- ▶ Avlytting
- ▶ Endring av informasjon
- ▶ Fabrikering/forfalskning

11174 Datasikkerhet

3. september 2002 Side 6

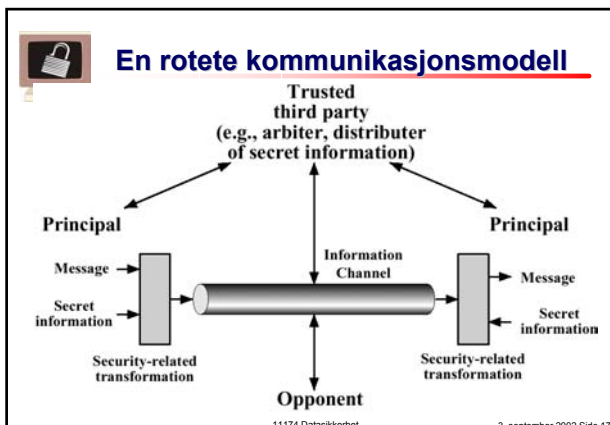




- ## Sikkerhetstjenester
- ▶ Konfidensialitet
 - ▶ Autentisering
 - ▶ Integritet
 - ▶ Ikke-fornektelse
 - ▶ Aksesskontroll
 - ▶ Tilgjengelighet
- 11174 Datasikkerhet 3. september 2002 Side 14

- ## Ikke-fornektelse (nonrepudiation)
- ▶ Av avgjørende betydning i finansverden
 - ▶ Budrunder ved huskjøp
 - ▶ "Jeg bød da ikke mer enn 900 000!"
 - ▶ Kjøp/salg av aksjer
 - ▶ "Jeg mente at jeg skulle ha EN Telenor-aksje, ikke en million!"
- 11174 Datasikkerhet 3. september 2002 Side 15

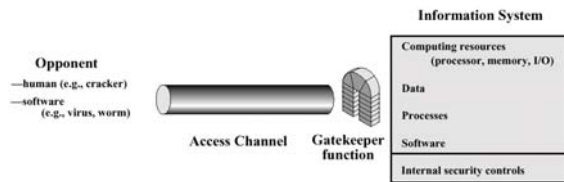
- ## Aksesskontroll
- ▶ Evnen til å begrense og kontrollere tilgang til datamaskinsystemer over kommunikasjonsforbindelser
 - ▶ Brukes også internt i et system
- 11174 Datasikkerhet 3. september 2002 Side 16



- ## Konstruksjon av sikkerhetstjenester
- ▶ Konstruer en algoritme for sikkerhets-transformasjonen
 - ▶ Generér den hemmelige informasjonen som skal brukes med algoritmen
 - ▶ Utvikl metoder for distribusjon av den hemmelige informasjonen
 - ▶ Angi en protokoll som bruker algoritmen og den hemmelige informasjonen
- 11174 Datasikkerhet 3. september 2002 Side 18



Sikkerhetsmodell for nettverksaksess

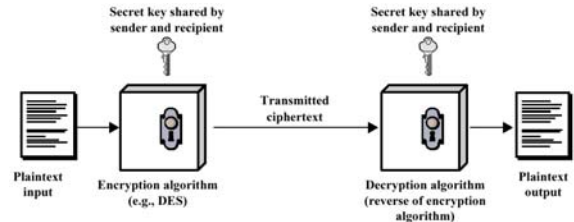


11174 Datasikkerhet

3. september 2002 Side 19



Konvensjonell kryptering

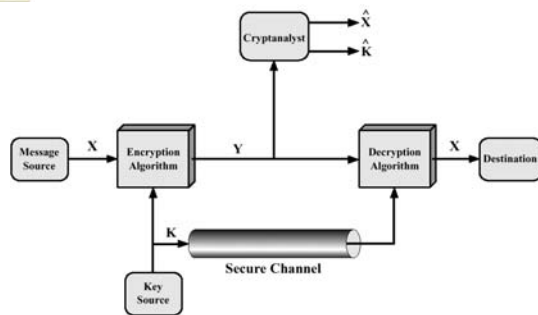


11174 Datasikkerhet

3. september 2002 Side 20



Konvensjonell krypteringsmodell



11174 Datasikkerhet

3. september 2002 Side 21



Notasjon

- ▶ X – klartekst
- ▶ K – nøkkel
- ▶ Y – chiffterkst (kryptert informasjon)
- ▶ E – kryptering
- ▶ D – dekryptering
- ▶ $Y = E_K(X)$
- ▶ $X = D_K(Y)$

11174 Datasikkerhet

3. september 2002 Side 22



Kryptografi

Kryptografiske systemer kjennetegnes ved:

- ▶ Hvilke typer operasjoner brukes for å transformere klartekst til chiffterkst
 - ▶▶ Substitusjon/permutasjon
- ▶ Antall nøkler som brukes
 - ▶▶ Symmetrisk/asymmetrisk
- ▶ Hvordan klarteksten behandles
 - ▶▶ Blokkchiffer/flytchiffer

11174 Datasikkerhet

3. september 2002 Side 23



Kerchoffs prinsipp

- ▶ Gå alltid ut fra at motstanderen vet hvilken algoritme som anvendes
- ▶ Sikkerheten i et kryptosystem avhenger ergo kun av *nøkkelen*
- ▶ Hvis man avviker fra dette, baserer man seg på "security through obscurity"

11174 Datasikkerhet

3. september 2002 Side 24



Kryptoanalyse

- ▶ Bare-chiffertekst
- ▶ Kjent klartekst
- ▶ Valgt klartekst
- ▶ Valgt chiffertekst
 - ▶ Asymmetriske algoritmer
- ▶ Det endelige målet er vanligvis nøkkelen

11174 Datasikkerhet

3. september 2002 Side 25



Steganografi

- ▶ Skjuling av informasjon i andre medier
- ▶ Ingen nøkkel
- ▶ Dette er ikke kryptografi!
- ▶ Eksempel:
 - ▶ Skjuling av data i diverse bildeformater
 - ▶ SNOW

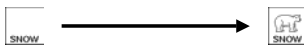
11174 Datasikkerhet

3. september 2002 Side 26



SNOW

- ▶ Steganographic Nature Of Whitespace
- ▶ <http://darkside.com.au>
- ▶ Informasjon i whitespace på slutten av linjer i ASCII tekst
- ▶ Logo: Hvitt har pixelverdi 255, isbjørnen tegnet med pixelverdi 254



11174 Datasikkerhet

3. september 2002 Side 27



Substitusjons-chiffer

- ▶ Cæsar
- ▶ Monoalfabetisk substitusjon
- ▶ Polyalfabetisk substitusjon - Vigenère

11174 Datasikkerhet

3. september 2002 Side 28



Cæsar

- ▶ Hver bokstav byttes ut med bokstaven som er (f.eks.) 3 plasser senere i alfabetet:
klartekst: a b c d e f g h i ...
chiffertekst: D E F G H I K L M ...
- ▶ $E_K(X) = (X+K) \bmod 29$ (for norsk alfabet)
- ▶ Finnes bare 28 mulige nøkler – knekkes trivielt ved å prøve alle

11174 Datasikkerhet

3. september 2002 Side 29



Monoalfabetisk substitusjon

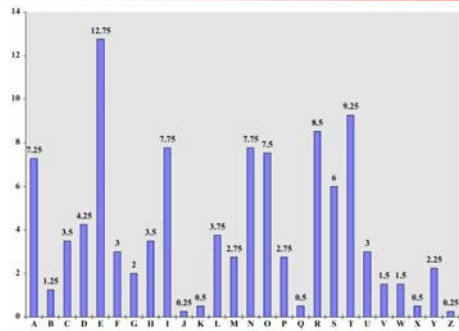
- ▶ Hver bokstav byttes ut med en vilkårlig valgt annen bokstav, eks. a→x, b→g, ...
- ▶ Nøkkelen er hele tabellen
- ▶ Finnes da $29! \approx 8,8 \cdot 10^{30}$ forskjellige nøkler (DES har $2^{56} \approx 7,2 \cdot 10^{16}$)
- ▶ Knekkes ved frekvensanalyse av chiffertekst
- ▶ Lange tekster enklere å knekke enn korte

11174 Datasikkerhet

3. september 2002 Side 30



Bokstavfordeling i engelsk tekst

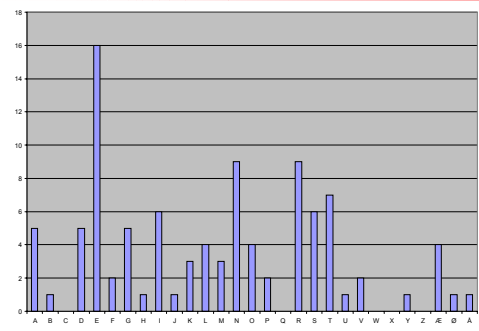


11174 Datasikkerhet

3. september 2002 Side 21



Bokstavfordeling i norsk tekst



11174 Datasikkerhet

3. september 2002 Side 22



Vigenère

- ▶ Baserer seg på alle mulige Cæsar-krypteringer
- ▶ Benytter seg av et repeterende nøkkelord for å velge aktuelt Cæsar-skift
- ▶ Eksempel: Kryptere "athlete" med nøkkelord "nerd"

11174 Datasikkerhet

3. september 2002 Side 33



Engelsk Vigenère-tabell

	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
a	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
b	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	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	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

11174 Datasikkerhet

3. september 2002 Side 34



Vigenère forts.

- ▶ $E_{nerd}(athlete) = NXYORXH$
- ▶ Legg merke til at de to e-ene blir forskjellige chiffrertekstbokstaver, mens de to t-ene blir begge X
 - ▶ Samme posisjon i forhold til nøkkelordet
athlete
nerdnerd

11174 Datasikkerhet

3. september 2002 Side 35



One-time pad

- ▶ Nøkkel like lang som klartekst
- ▶ Nøkkel fullstendig tilfeldig
- ▶ $Y = X \oplus K$, $X = Y \oplus K$
- ▶ Alle dekrypteringer er like sannsynlige
 - ▶ ksdhffklnkd kan like gjerne bety
 svaret er nei eller
 svaret er ja! eller
 Flåklypa i 90

11174 Datasikkerhet

3. september 2002 Side 36



Permutasjonschiffer

- ▶ Samme bokstaver beholdes i meldingen, men rekkefølgen byttes om
- ▶ Som ord-leker i barne-tv
- ▶ Mer avanserte varianter oppnås ved å fylle tekst i matriser radvis, permutere kolonner, og så skrive ut kolonnevis
- ▶ Permutasjon og substitusjon brukes som byggeklosser i mer avanserte algoritmer

11174 Datasikkerhet

3. september 2002 Side 27



Moderne teknikker

11174 Datasikkerhet



Moderne teknikker

- ▶ Prinsipper for blokkchiffer
- ▶ DES
- ▶ Differensiell/lineær kryptoanalyse
- ▶ Operasjonsmodi

11174 Datasikkerhet

3. september 2002 Side 39



Feistel-chiffer

- ▶ En sikker kryptering vil være en $n \times n$ bits blokk-substitusjon
- ▶ Imidlertid medfører fornuftig blokk-størrelse veldig ufornuftig nøkkellengde (4 bits blokk \Rightarrow 64 bits nøkkel)
- ▶ Ved å kombinere enklere chifre kan man tilnærme "det ideelle chiffer" med kortere nøkkellengder.

11174 Datasikkerhet

3. september 2002 Side 40



Feistel forts.

- ▶ *Diffusion*
 - ▶▶ (Mangel på) sammenheng mellom klartekst og chiffterkst
- ▶ *Confusion*
 - ▶▶ (Mangel på) sammenheng mellom chiffterkst og nøkkel
- ▶ Hensikten er å unngå statistiske sammenhenger mellom klartekst og chiffterkst

11174 Datasikkerhet

3. september 2002 Side 41



Avalanche-effekt

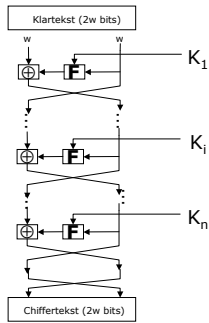
- ▶ En ønsket egenskap til en krypto-algoritme er at en liten endring i nøkkel eller klartekst skal medføre en stor endring i chiffterkst
- ▶ Eks: Forandring av en bit i nøkkelen medfører at halvparten av bitene i chiffterksten endres

11174 Datasikkerhet

3. september 2002 Side 42



Klassisk (n-round) Feistel nettverk



11174 Dataikkerhet 3. september 2002 Side 43



Hvorfor en ekstra SW?

- ▶ Årsaken til at de to halvpartene av output byttes om på slutten av algoritmen, er at dette muliggjør at samme algoritmen kan brukes til dekryptering ved å bruke nøklene i omvendt rekkefølge.
- ▶ Grunnen til at det er to ombyttinger etter hverandre er at det er enklest å betrakte "SW" som en del av hver runde - da blir den siste runden lik de andre

11174 Dataikkerhet 3. september 2002 Side 44



The Data Encryption Standard

- ▶ Utviklet av IBM med "hjelp" fra NSA
- ▶ Akseptert som standard i 1977
- ▶ Mest kjent av alle Feistel-chifre
- ▶ 64 bit blokkstørrelse, 56 bit nøkkel
- ▶ Brukt som standard i mange applikasjoner
- ▶ Ikke lenger regnet som sterk nok mot "brute force"

11174 Dataikkerhet 3. september 2002 Side 45



Moderne kryptoanalyse

- ▶ Differensiell
 - ▶▶ For å knekke DES kreves 2^{47} valgte klartekster
- ▶ Lineær
 - ▶▶ For å knekke DES kreves 2^{47} kjente klartekster

11174 Dataikkerhet 3. september 2002 Side 46



Moderne Brute-Force

- ▶ EFF "Deep Crack" kan knekke DES "brute force" i løpet av noen dager
- ▶ Distributed.Net i samarbeid med EFF løste DES-III konkurransen i løpet av 22 timer

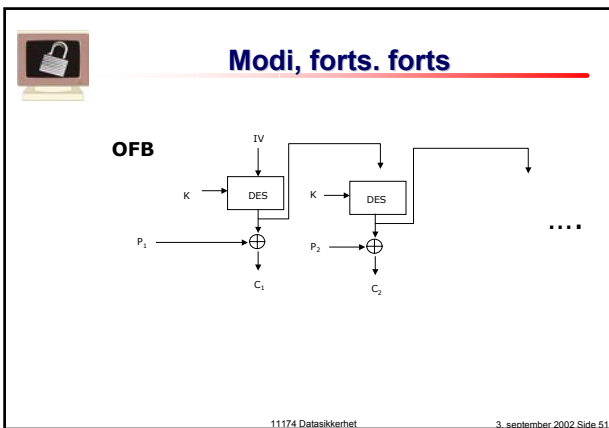
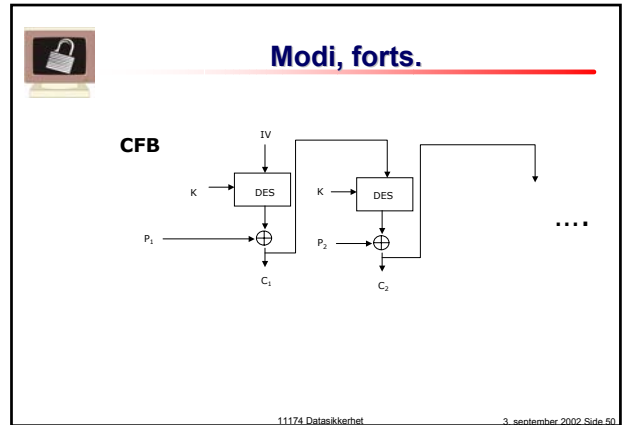
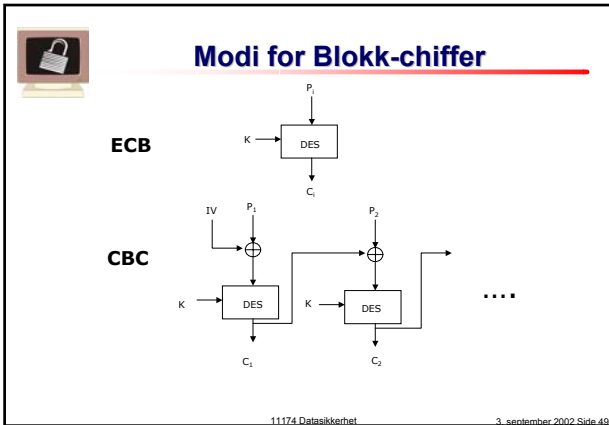
11174 Dataikkerhet 3. september 2002 Side 47



Design-kriterier

- ▶ Avalanche-effekten
- ▶ Motstandsdyktighet mot differensiell kryptoanalyse
- ▶ Antall runder
 - ▶▶ Gjør kryptoanalyse vanskeligere enn "brute force"

11174 Dataikkerhet 3. september 2002 Side 48



Dagens website

► <http://www.counterpane.com>

11174 Datasikkerhet 3. september 2002 Side 52