



Forelesning 3

Konvensjonell kryptering:
Algoritmer
Konfidensialitet



De mest brukte algoritmene idag

- ▶ Triple DES
 - ▶ IDEA
 - ▶ Blowfish
 - ▶ RC5
 - ▶ CAST
 - ▶ RC2
- Kommer:
AES

11174 Datasikkerhet

9. september 2002 Side 2



En liten advarsel

- ▶ Stallings bruker til enhver tid samme notasjon som designeren av en gitt algoritme har brukt i sin beskrivelse
- ▶ Intet forsøk på en enhetlig notasjon i beskrivelsene!
- ▶ Caveat studiosis!

11174 Datasikkerhet

9. september 2002 Side 3



DES har for kort nøkkel!

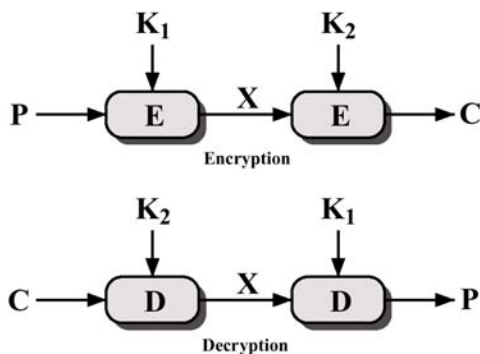
- ▶ Dette har vært akseptert lenge, selv om det er bare i de senere årene at vi har sett at DES kan knekkes i praksis i løpet av et fåtall timer
- ▶ Ønskelig å utnytte det som fantes av hardware og infrastruktur for DES til å tilby en algoritme med økt nøkkellengde

11174 Datasikkerhet

9. september 2002 Side 4



Double DES



11174 Datasikkerhet

9. september 2002 Side 5



Hva med Double DES ?

- ▶ $C = E_{K_2}[E_{K_1}(P)]$
- ▶ $56+56 = 112$ bits nøkkel
- ▶ $\exists K_3 \mid E_{K_3}[P] = E_{K_1}[E_{K_2}(P)]$?
- ▶ Alle permutasjoner av 64 bit:
 $(2^{64})! > 10^{10^{20}}$ mappinger
- ▶ En mapping pr nøkkel:
 $2^{56} < 10^{17}$ mappinger
- ▶ Ingen slik K_3 finnes!

11174 Datasikkerhet

9. september 2002 Side 6



Meet-in-the-middle angrep

- ▶ $C = E_{K_2}[E_{K_1}(P)]$
- ▶ $X = E_{K_1}[P] = D_{K_2}[C]$
- ▶ Med et kjent (P,C) par:
 - ▶▶ Krypter P med alle 2^{56} mulige K_1
 - ▶▶ Dekrypter C med alle 2^{56} mulige K_2
 - ▶▶ For hver dekrypterte C, sjekk for match med kryptert P

11174 Datasikkerhet

9. september 2002 Side 7



Meet-in-the-middle eksempel

K_1	$E_{K_1}[P]$	$D_{K_2}[C]$	K_2
1	a	z	i
2	b	h	ii
3	c	p	iii
4	d	q	iv
5	e	b	v
6	f	t	vi
...

11174 Datasikkerhet

9. september 2002 Side 8



Meet-in-the-middle forts.

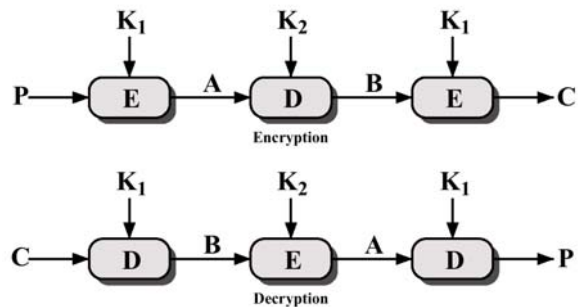
- ▶ Prosedyren gir 2^{48} falske alarmer med ett kjent (P,C) par
- ▶ Med to kjente (P,C) par finner man rett nøkkel med en sannsynlighet på $1-2^{-16} = 0,999985$
- ▶ Kan knekke Double-DES med kjent klartekst med $\approx 4 * 2^{56}$ operasjoner (mye dårligere enn de 2^{112} vi kanskje kunne forvente)

11174 Datasikkerhet

9. september 2002 Side 9



Triple DES



11174 Datasikkerhet

9. september 2002 Side 10



Triple DES

- ▶ Tre nøkler ansett som u håndterlig, to nøkler kompromiss
- ▶ Krypter med den første nøkkelen, dekrypter med den andre, og så krypter med den første igjen
- ▶ $C = E_{K_1}[D_{K_2}(E_{K_1}[P])]$
- ▶ Nøkkellengde $56+56 = 112$ bit
- ▶ Mye bedre motstand mot m-i-t-m

11174 Datasikkerhet

9. september 2002 Side 11



IDEA

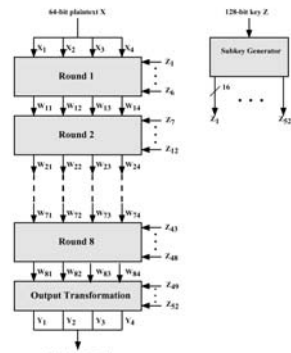
- ▶ International Data Encryption Algorithm
- ▶ 128 bit nøkkellengde
- ▶ 64 bit blokk lengde
- ▶ 16-bits operasjoner internt
- ▶ IKKE et Feistel-chiffer!

11174 Datasikkerhet

9. september 2002 Side 12



Oversikt over IDEA



11174 Datasikkerhet 9. september 2002 Side 13



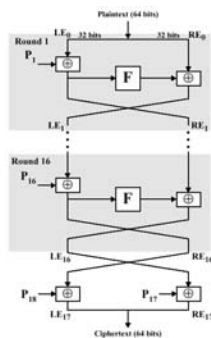
Blowfish

- ▶ 32 til 448 (=14*32) bit nøkkellengde
- ▶ 64 bit blokk lengde
- ▶ 16 runder
- ▶ 32-bits operasjoner internt
- ▶ Nøkkelavhengige S-bokser
- ▶ "Feistel-aktig"

11174 Datasikkerhet 9. september 2002 Side 14



Blowfish kryptering



11174 Datasikkerhet 9. september 2002 Side 15



Blowfish betraktninger

- ▶ Operasjoner gjøres på begge halvdelene av data i hver runde
- ▶ Brute-force gjøres "umulig" pga. den nøkkelavhengige oppbyggingen av S-boksene
- ▶ Etter at P,S er klar (kan beregnes på forhånd for gitt nøkkel) er Blowfish meget rask

11174 Datasikkerhet 9. september 2002 Side 16



RC5

- ▶ 0 til 255 byte nøkkel
- ▶ 32 til 128 bit blokkstørrelse
- ▶ 0 til 255 runder
- ▶ Variabel bitstørrelse internt
- ▶ IKKE et Feistel-chiffer

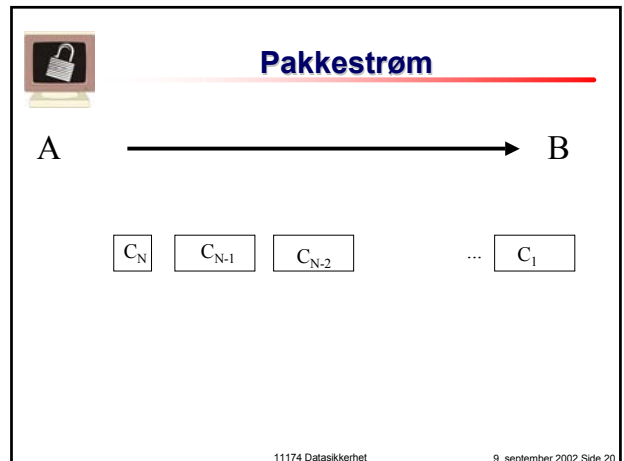
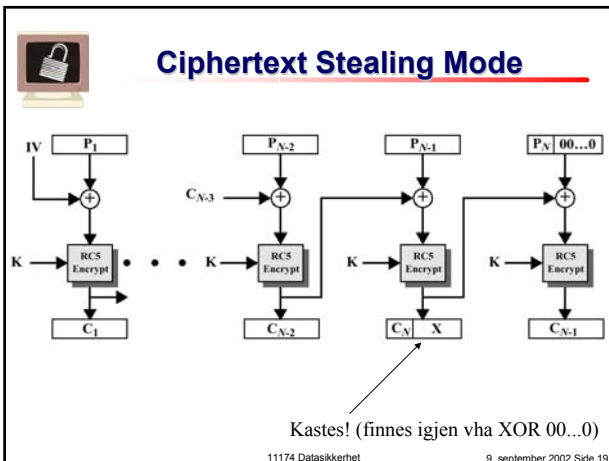
11174 Datasikkerhet 9. september 2002 Side 17



RC5 modi

- ▶ RC5 Block – ECB
- ▶ RC5-CBC
- ▶ RC5-CBC-Pad – CBC med padding
- ▶ RC5-CTS

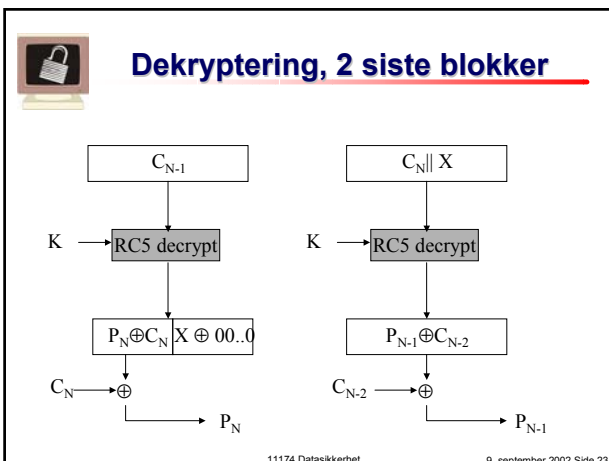
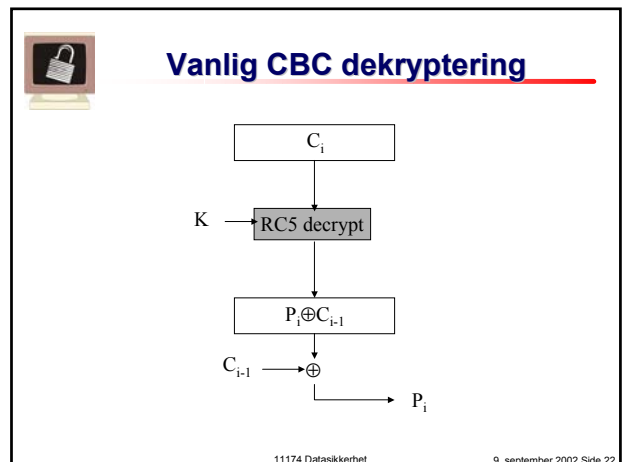
11174 Datasikkerhet 9. september 2002 Side 18



Dekryptering

- ▶ B må vite at ciphertext stealing er utført, og må derfor stoppe dekryptering når han kommer til den NEST siste blokken
- ▶ De to siste blokkene må behandles spesielt

11174 Datasikkerhet 9. september 2002 Side 21



Hva er poenget?

- ▶ Ved å bruke Ciphertext Stealing Mode slipper man å sende flere bit enn man faktisk har i meldingen ut på nettet

11174 Datasikkerhet 9. september 2002 Side 24



CAST-128

- ▶ 40 til 128 bit nøkkellengde
- ▶ 64 bit blokk lengde
- ▶ 16 runder
- ▶ 32 bit operasjoner internt
- ▶ Feistel-struktur
- ▶ Runde-avhengig F

11174 Datasikkerhet

9. september 2002 Side 25



Blokkchiffer oppsummering

	Nøkkel	Blokk	Runder	Internt	Spesial
3-DES	112 (168)	64	48	32	EDE
IDEA	128	64	8	16	Ikke Feistel
Blowfish	32-448	64	16	32	Nøkkelavh. S-boks
RC5	0-255*8	32-128	0-255	Var.	Ikke Feistel
CAST-128	40-128	64	16	32	Rundeavh.o peratorer
RC2	8-1024	64	18	16	Absolutt ikke Feistel

11174 Datasikkerhet

9. september 2002 Side 26



Hastighet Algoritmer (Pentium)

Algoritme	Klokkesyklus per runde	Antall runder	Klokkesyklus per byte kryptert
Blowfish	9	16	18
RC5	12	16	23
DES	18	16	45
IDEA	50	8	50
Triple-DES	18	48	108

11174 Datasikkerhet

9. september 2002 Side 27



Karakteristikk

Følgende karakteristikk gjelder i større eller mindre grad for moderne blokkchiffer:

- ▶ Variabel nøkkellengde
- ▶ Flere primitive operasjoner
- ▶ Data-avhengig rotasjon
- ▶ Nøkkel-avhengig rotasjon
- ▶ Nøkkel-avhengig S-bokser

11174 Datasikkerhet

9. september 2002 Side 28



Karakteristikk, forts.

- ▶ Lang "key schedule" algoritme
- ▶ Variabel F-funksjon
- ▶ Variabel blokk lengde
- ▶ Variabelt antall runder
- ▶ Operasjon på begge halvpartene av data i hver runde

11174 Datasikkerhet

9. september 2002 Side 29



Konfidensialitet ved hjelp av konvensjonell kryptering



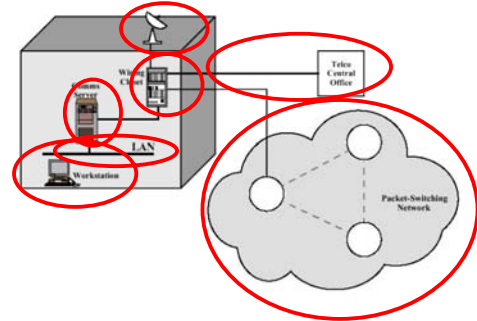
Hvor finnes truslene?

- ▶ Lokal maskin
- ▶ Lokalt nettverk (LAN)
- ▶ Oppringt samband
- ▶ Koblingsskap
- ▶ Eksternt nettverk

11174 Datasikkerhet 9. september 2002 Side 31



Svake punkter

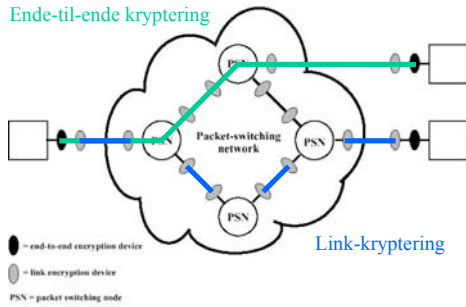


11174 Datasikkerhet 9. september 2002 Side 32



Link vs Ende-til-ende kryptering

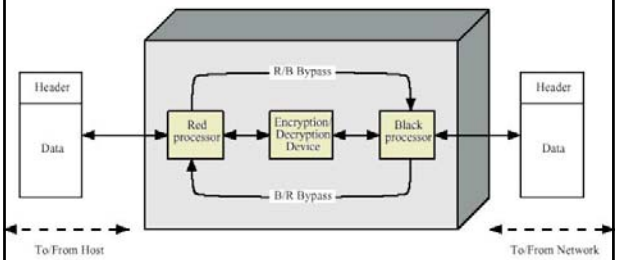
Ende-til-ende kryptering



11174 Datasikkerhet 9. september 2002 Side 33



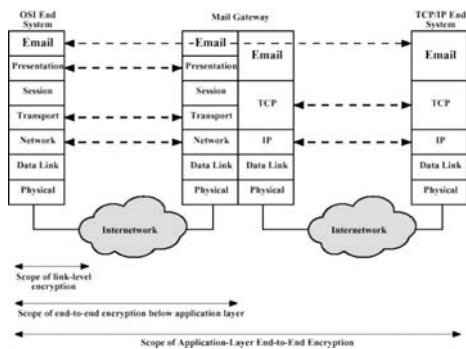
Front End Processor (FEP)



11174 Datasikkerhet 9. september 2002 Side 34



Kryptering på ulike nivåer



11174 Datasikkerhet 9. september 2002 Side 35



Trusselevuering

Transitt	Link-H	Net-H	IP-H	TCP-H	Data	Link-T
Node	Link-H	Net-H	IP-H	TCP-H	Data	Link-T

APPLICATION LEVEL ENCRYPTION

Transitt	Link-H	Net-H	IP-H	TCP-H	Data	Link-T
Node	Link-H	Net-H	IP-H	TCP-H	Data	Link-T

TCP LEVEL ENCRYPTION

Transitt	Link-H	Net-H	IP-H	TCP-H	Data	Link-T
Node	Link-H	Net-H	IP-H	TCP-H	Data	Link-T

LINK LEVEL ENCRYPTION

11174 Datasikkerhet 9. september 2002 Side 36



Trafikkanalyse

- ▶ Identitet til partnere
- ▶ Hvor ofte kommuniserer partnere?
- ▶ Trafikkmønster, meldingslengder eller meldingsmengde kan indikere viktighet
- ▶ Begivenheter som korrelerer med spesielle konversasjoner mellom spesielle partnere

11174 Datasikkerhet

9. september 2002 Side 37



Covert Channel

- ▶ Bruk av en kommunikasjonskanal på en måte som ikke var tiltenkt av designerne
- ▶ F.eks. definere at meldinger fra A til B større enn 20kB betyr "1" og meldinger mindre enn 20kB betyr "0"
- ▶ Overvåkning av dataene mellom A og B vil ikke avsløre den skjulte dataflyten
- ▶ Også: Variable forsinkelser, etc.

11174 Datasikkerhet

9. september 2002 Side 38



Padding

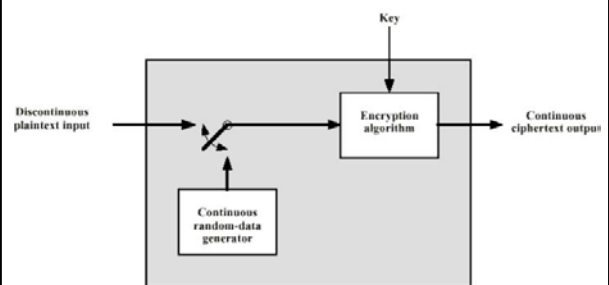
- ▶ Kan brukes for å forhindre trafikkanalyse
- ▶ Mest aktuelt for link-kryptering
- ▶ Medfører konstant datarate mellom alle noder
- ▶ Kan i gitte tilfeller også forhindre "covert channels"

11174 Datasikkerhet

9. september 2002 Side 39



Traffic Padding



11174 Datasikkerhet

9. september 2002 Side 40



Nøkkeldistribusjon

- ▶ For at to parter skal kunne kommunisere vha. konvensjonell kryptering, må begge ha den samme nøkkelen
- ▶ Hvordan oppnår man dette?

11174 Datasikkerhet

9. september 2002 Side 41



Nøkkeldistribusjon

- ▶ A velger en nøkkel, og leverer den manuelt til B
- ▶ En tredjepart velger en nøkkel for A og B, og leverer den manuelt til dem
- ▶ A kan velge en nøkkel og sende den til B kryptert med en tidligere nøkkel
- ▶ Hvis A og B begge har en kryptert forbindelse til C, kan C sende en kryptert nøkkel til hver av dem

11174 Datasikkerhet

9. september 2002 Side 42



Nøkkelantall

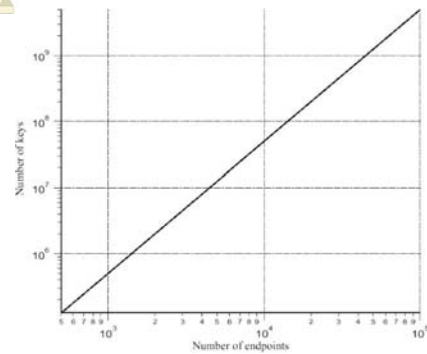
- ▶ Hvis N maskiner skal kommunisere med hverandre, trenger man

$$\frac{N(N-1)}{2}$$

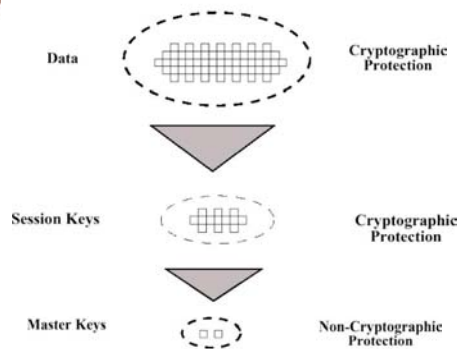
nøkler



Nøkkelantall illustrert



Nøkkelhierarki

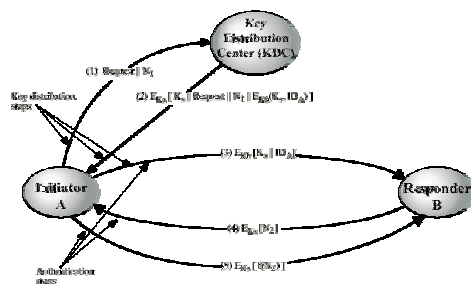


Nøkkeldistribusjon vha. KDC

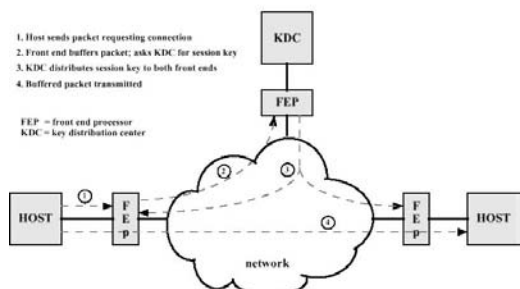
- ▶ A deler en nøkkel K_a med KDC
- ▶ B deler en nøkkel K_b med KDC
- ▶ KDC velger sesjonsnøkkel K_s
- ▶ A velger tilfeldig tall (nonce) N_1
- ▶ B velger tilfeldig tall (nonce) N_2



Nøkkeldistribusjon-scenario

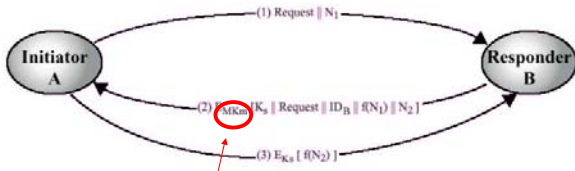


Transparent nøkkeldistribusjon





Desentralisert nøkkeldistribusjon



Må ha en delt Master Key med alle kommunikasjonspartnere!

11174 Datasikkerhet

9. september 2002 Side 49



Rett nøkkel på rett sted

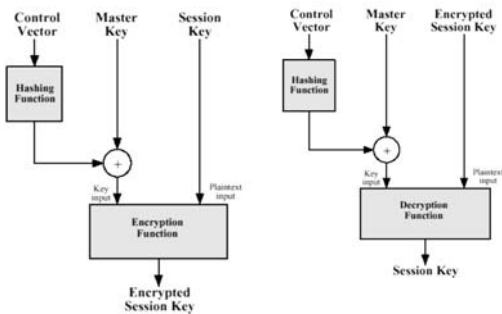
- ▶ Et nøkkelhierarki forutsetter at nøklene brukes som forventet
- ▶ Hvis f.eks. en "master key" brukes til å kryptere en større datastrøm, vil den være betraktelig mer sårbar for kryptoanalyse, noe som truer hele hierarkiet
- ▶ Kan være ønskelig å "merke" nøkler med forventet bruksområde

11174 Datasikkerhet

9. september 2002 Side 50



Control Vector Coupling



11174 Datasikkerhet

9. september 2002 Side 51



Tilfeldige tall

- ▶ Autentisering basert på nonce (forhindrer replay)
- ▶ Sesjonsnøkkel-generering
- ▶ Generering av RSA-nøkler

11174 Datasikkerhet

9. september 2002 Side 52



Krav til tilfeldige tall

- ▶ "Randomitet"
 - ▶▶ Uniform fordeling
 - ▶▶ Uavhengighet
- ▶ Uforutsigbarhet
- ▶ Oftest sier man seg tilfreds med tall som er "pseudo-random"

11174 Datasikkerhet

9. september 2002 Side 53



The Linear Congruential Method

- ▶ Velg $m \mid m > 0$
- ▶ Velg $a \mid 0 \leq a < m$
- ▶ Velg $c \mid 0 \leq c < m$
- ▶ Velg $X_0 \mid 0 \leq X_0 < m$
- ▶ $X_{n+1} = (aX_n + c) \bmod m$
- ▶ Ikke uforutsigbar!

11174 Datasikkerhet

9. september 2002 Side 54



Kriterier for random-funksjoner

- ▶ Funksjonen må generere en full periode
- ▶ Sekvensen må se tilfeldig ut
- ▶ Funksjonen må kunne implementeres effektivt

11174 Datasikkerhet

9. september 2002 Side 55



Kryptografisk generering

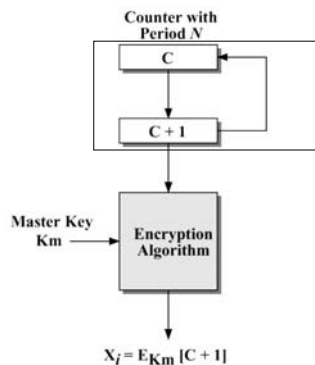
- ▶ Syklisk kryptering
- ▶ DES OFB
- ▶ ANSI X9.17

11174 Datasikkerhet

9. september 2002 Side 56



Syklisk kryptering



9. september 2002 Side 57



ANSI X9.17

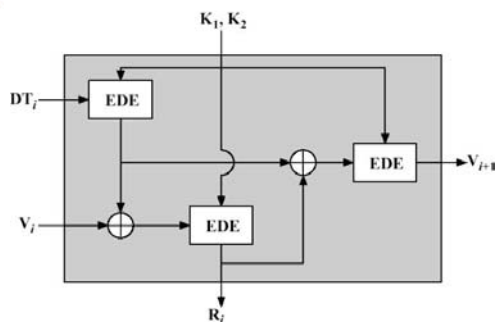
- ▶ Input
 - ▶▶ DT_i – 64-bits representasjon av dato og tid
 - ▶▶ V_i – 64 bits "seed"
 - ▶▶ K_1, K_2 – Triple-DES-nøkler
- ▶ Output
 - ▶▶ R_i – 64-bits pseudorandom tall
 - ▶▶ V_{i+1} – 64-bits "seed" til neste runde

11174 Datasikkerhet

9. september 2002 Side 58



ANSI X9.17



11174 Datasikkerhet

9. september 2002 Side 59



Dagens website

- ▶ <http://www.securityfocus.com>

11174 Datasikkerhet

9. september 2002 Side 60