Forelesning 2

Introduksjon til nettverkssikkerhet

Tre fundamenter 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

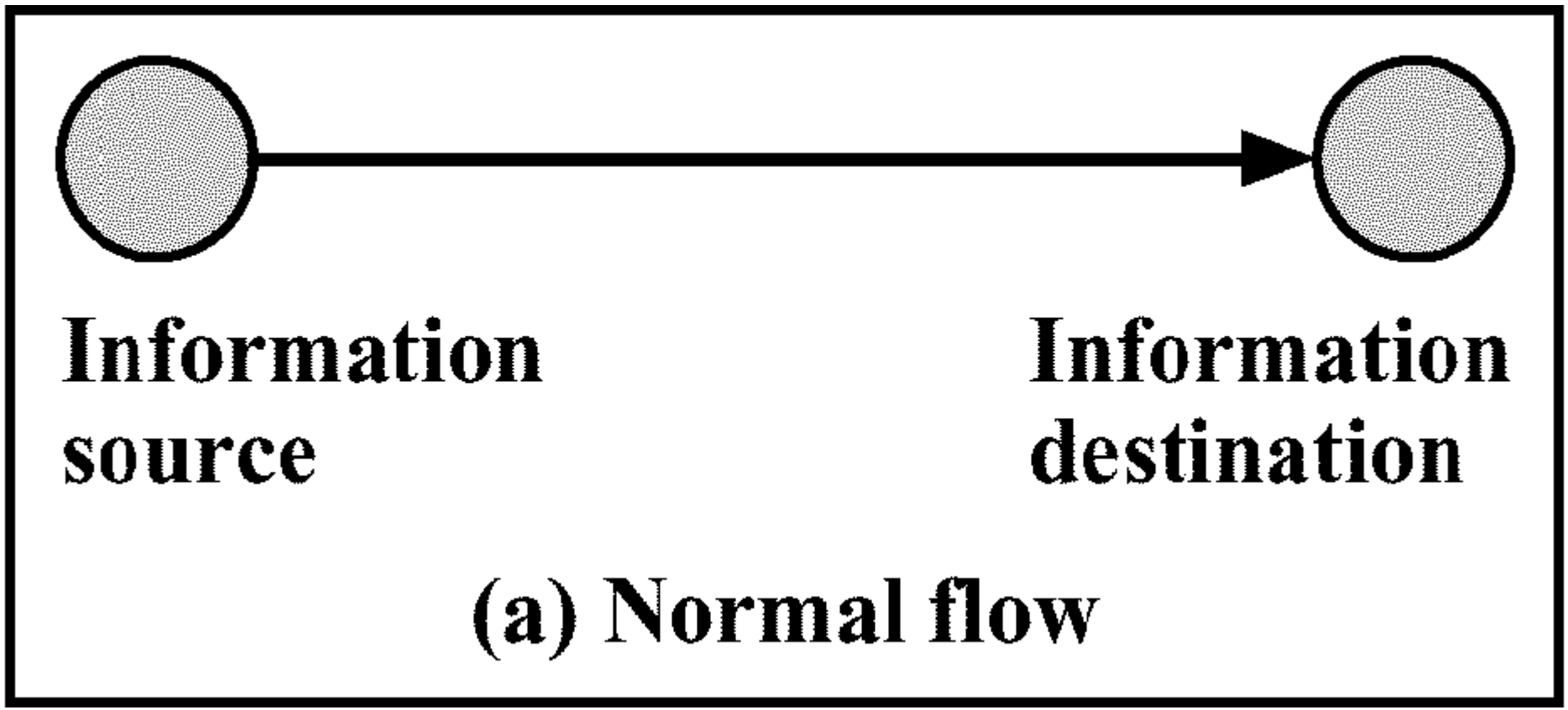
... som igjen hviler på

- 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?

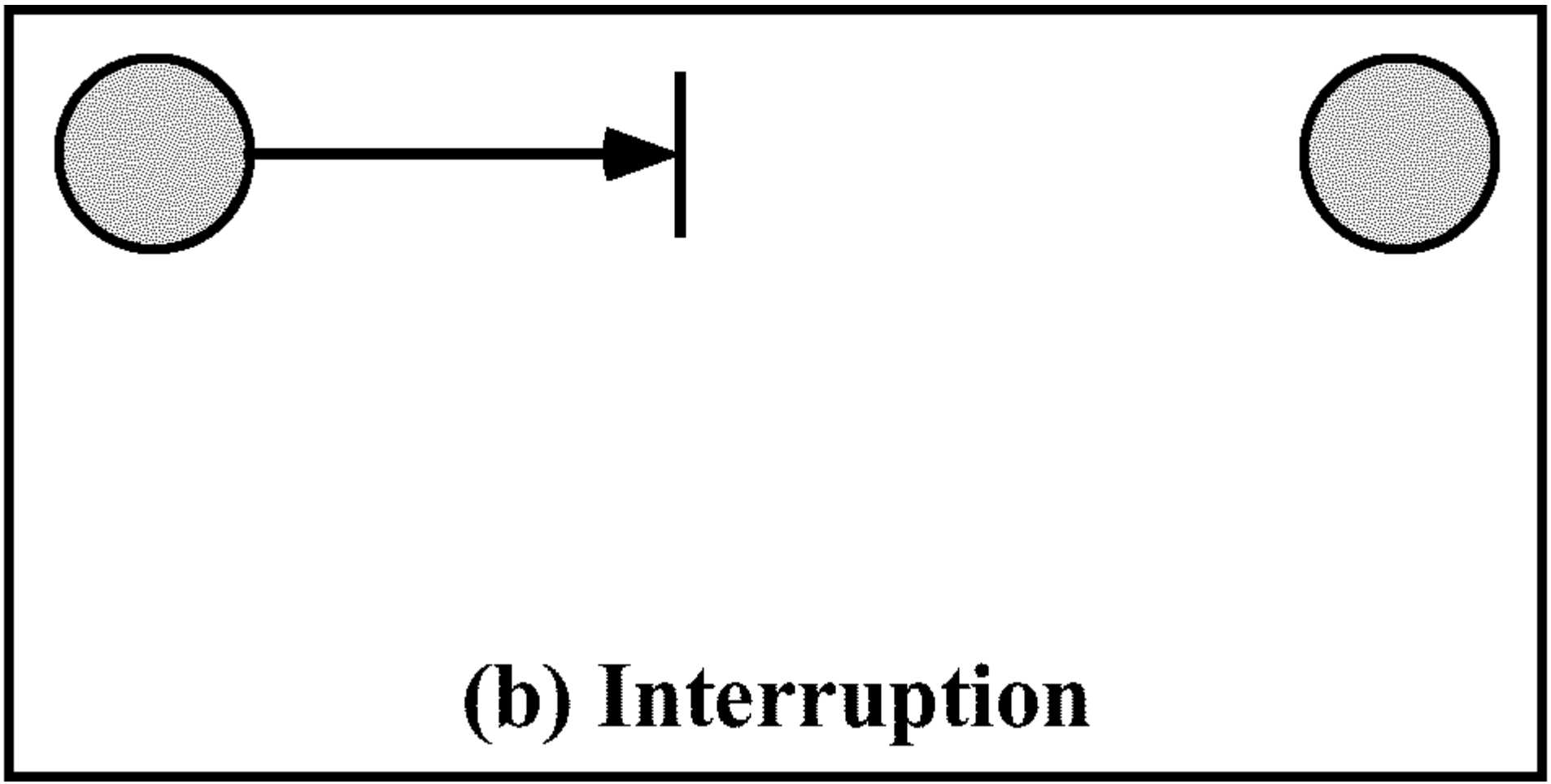
Sikkerhetstrusler

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

Normal trafikkflyt

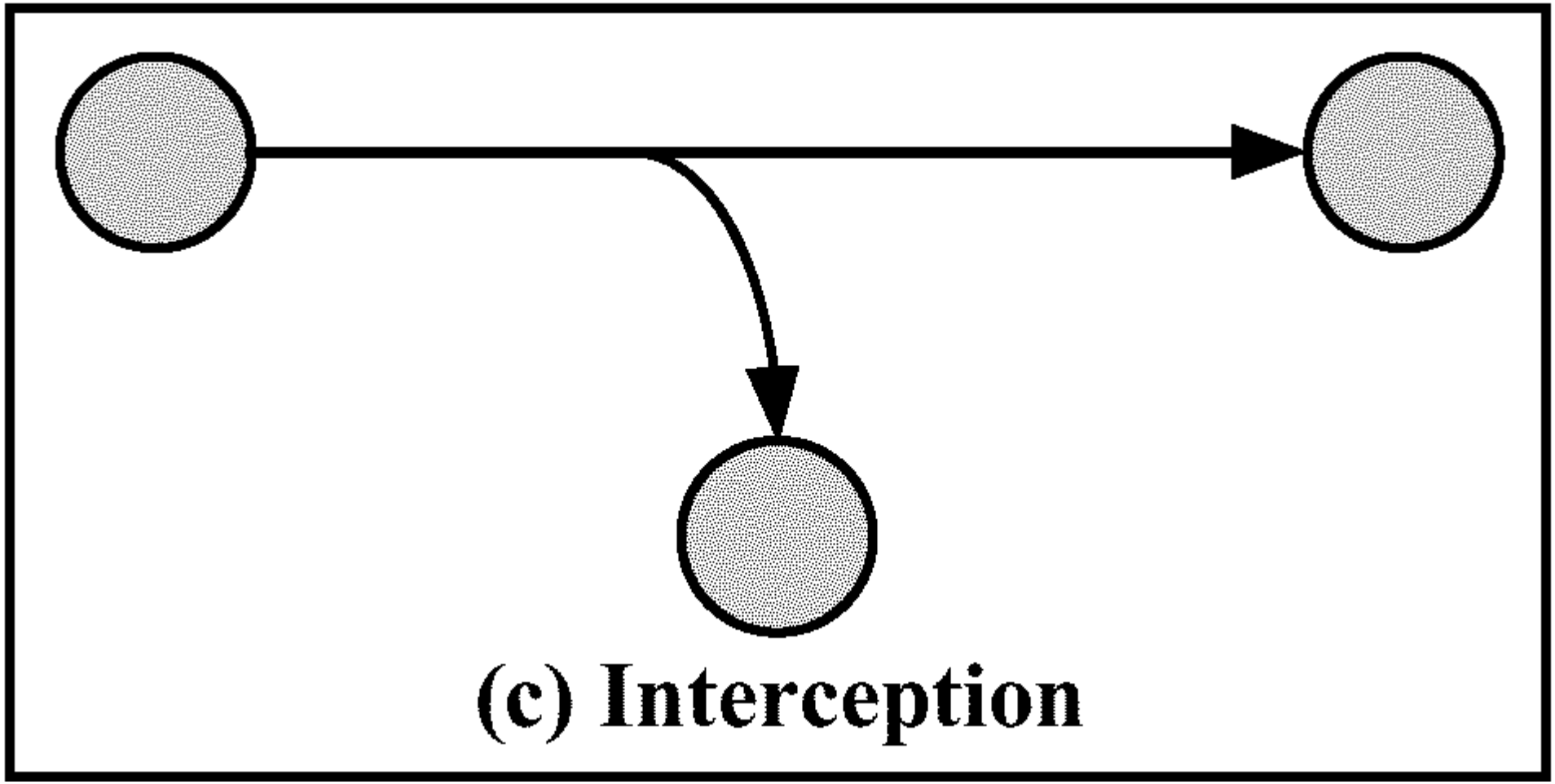


Kommunikasjonsbrudd

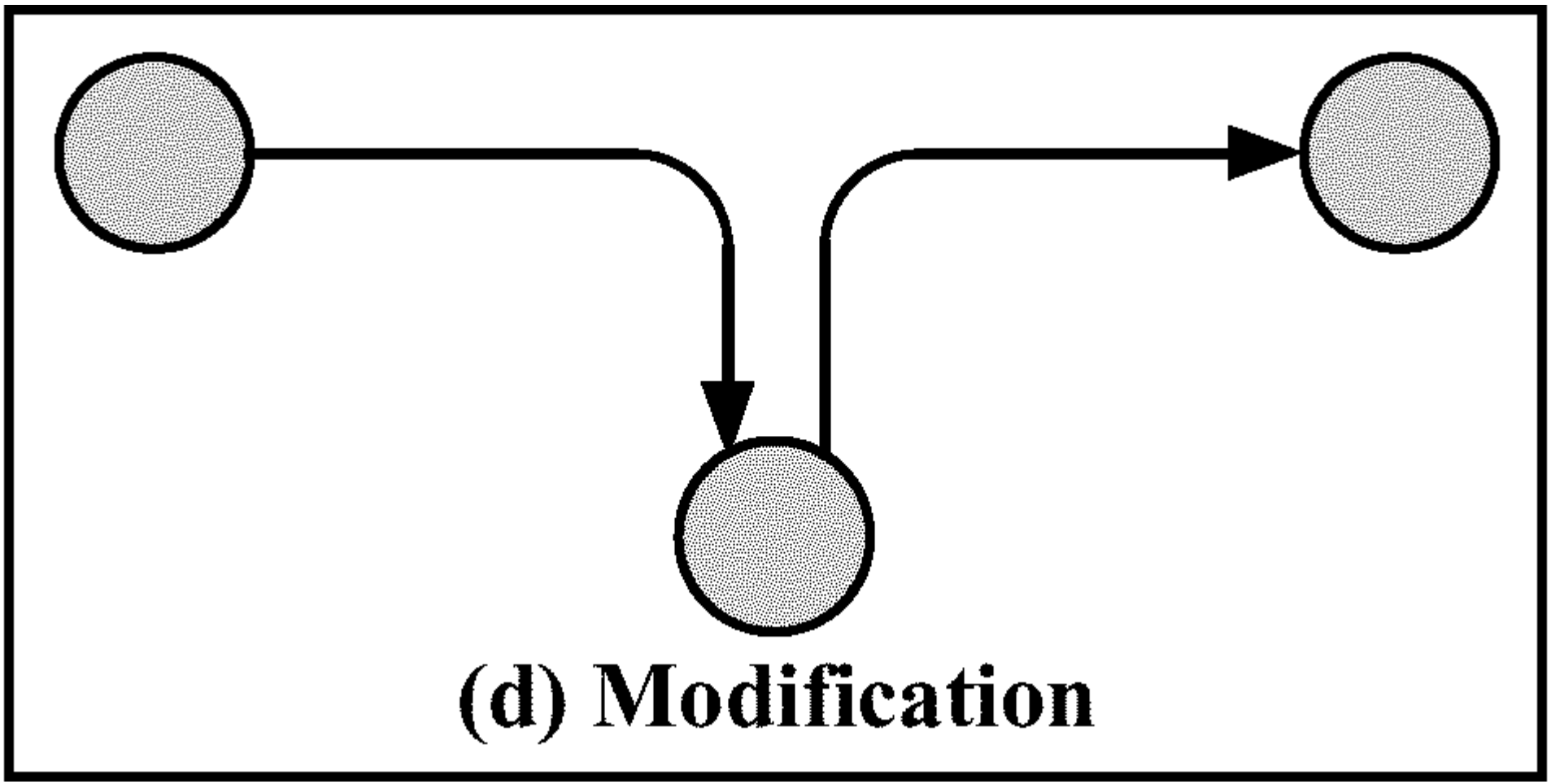


(b) Interruption

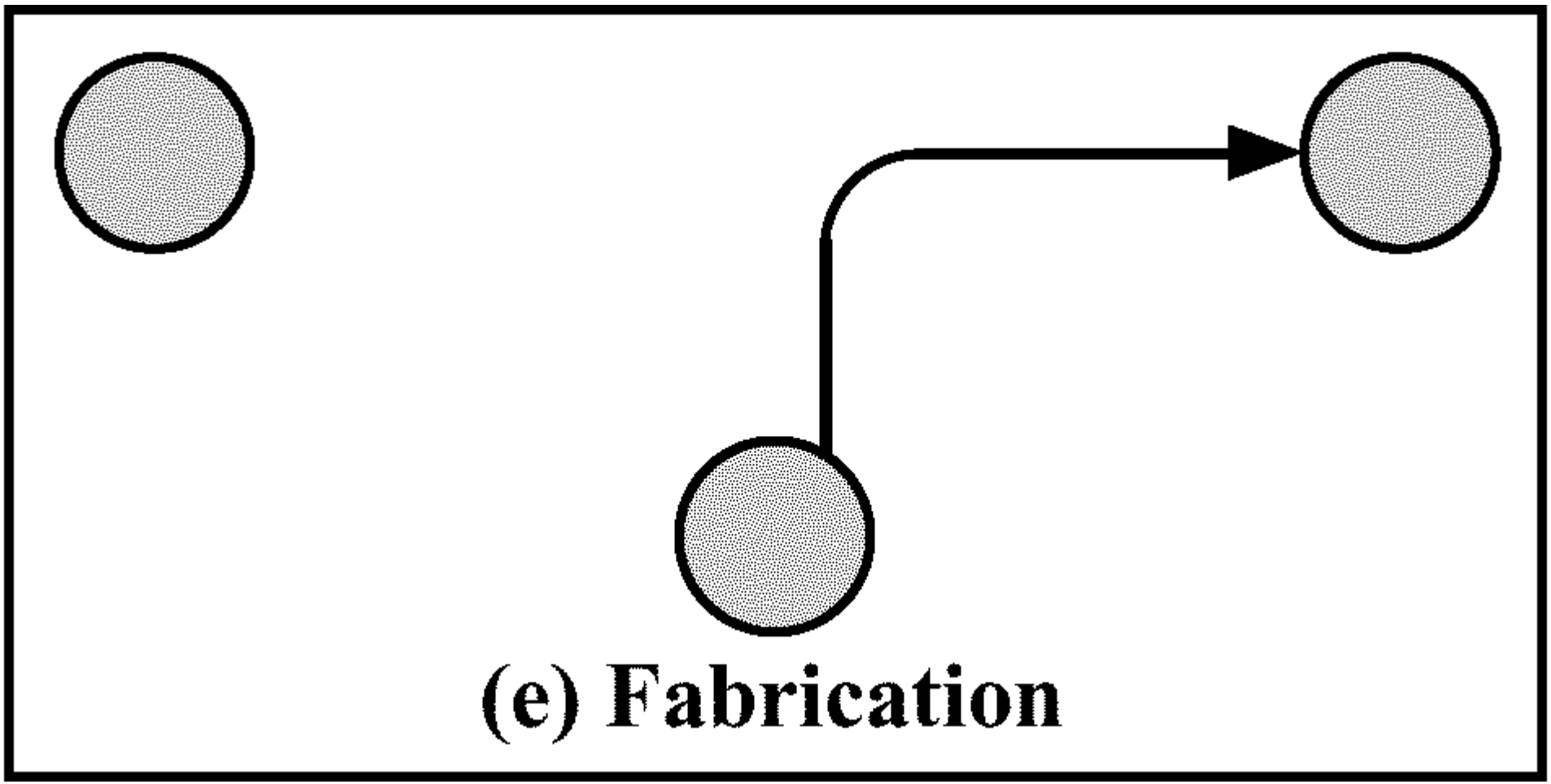
Avlytting



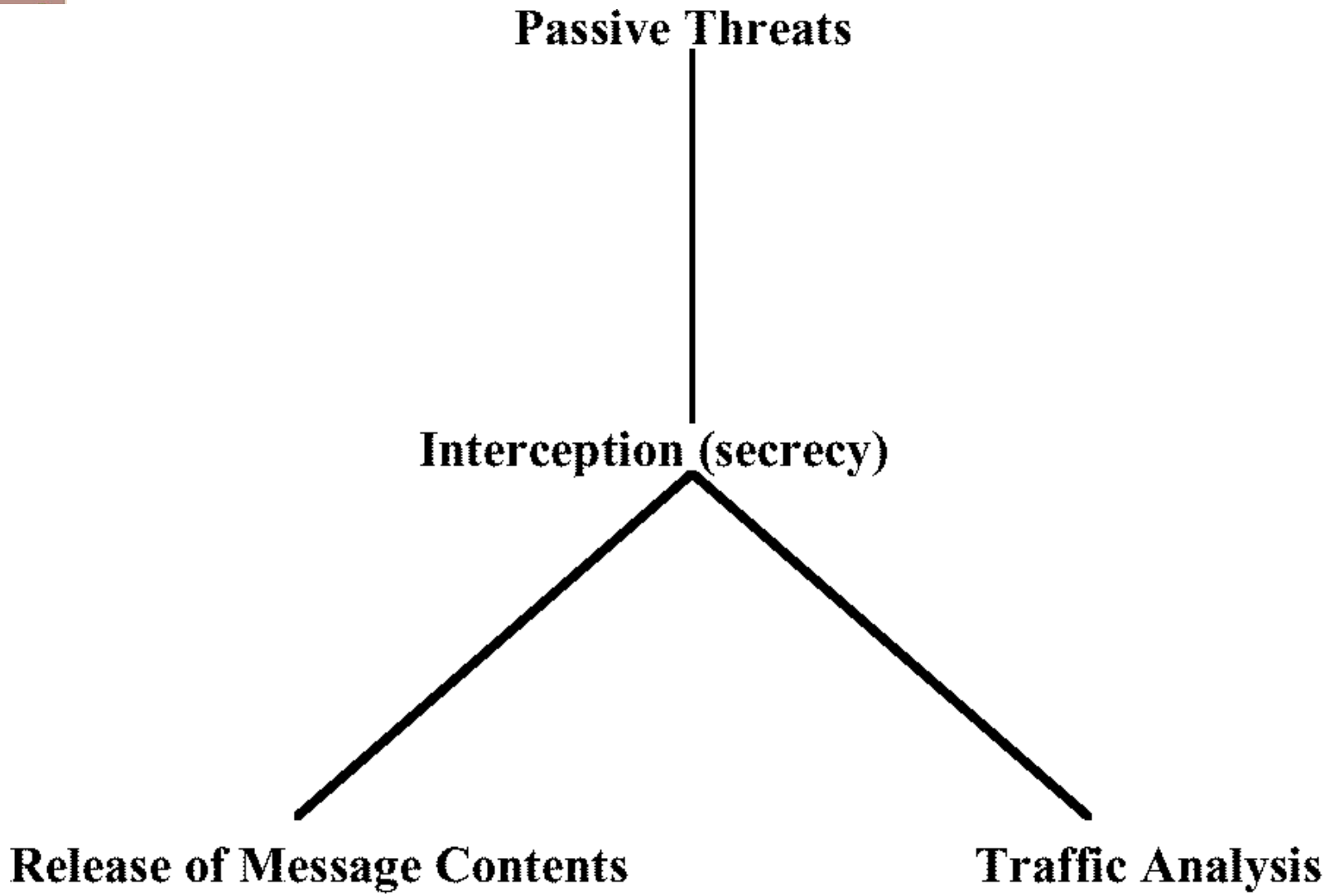
Endring av informasjon



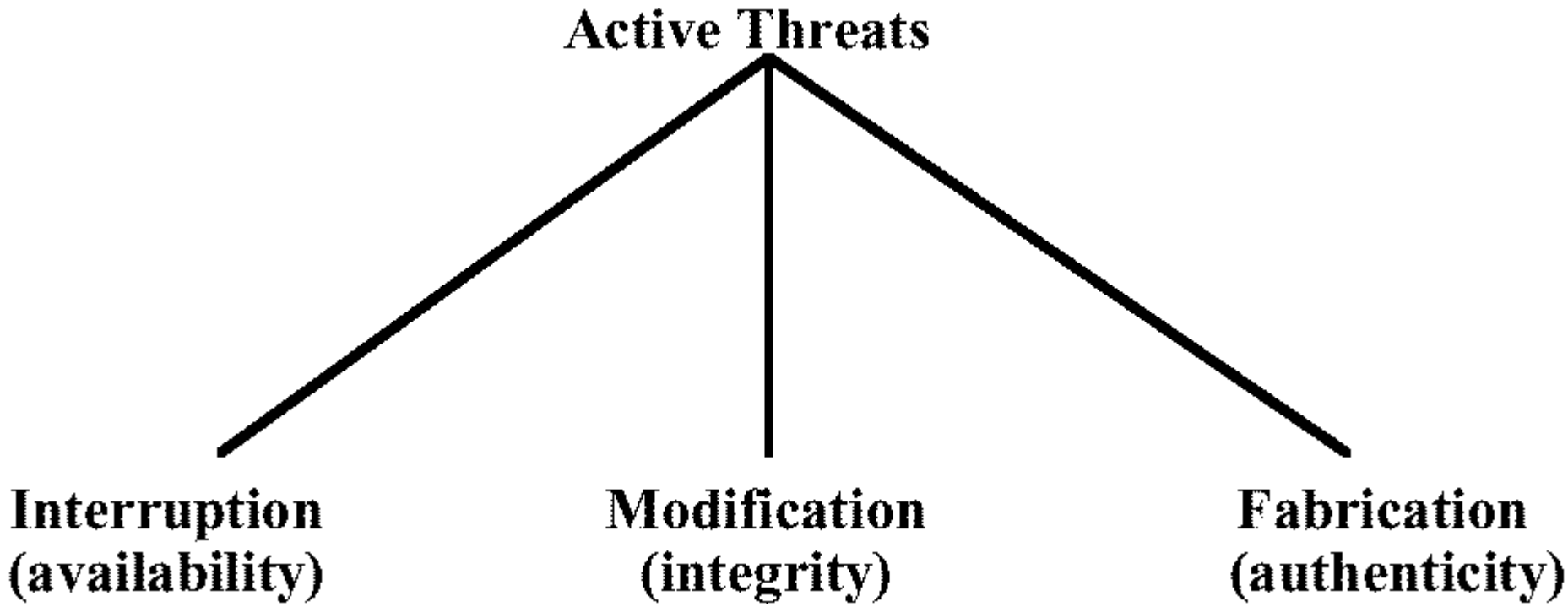
Fabrikering



Passive trusler



Aktive trusler



Sikkerhetstjenester

- Konfidensialitet
- Autentisering
- Integritet
- Ikke-fornektelse
- Aksesskontroll
- Tilgjengelighet

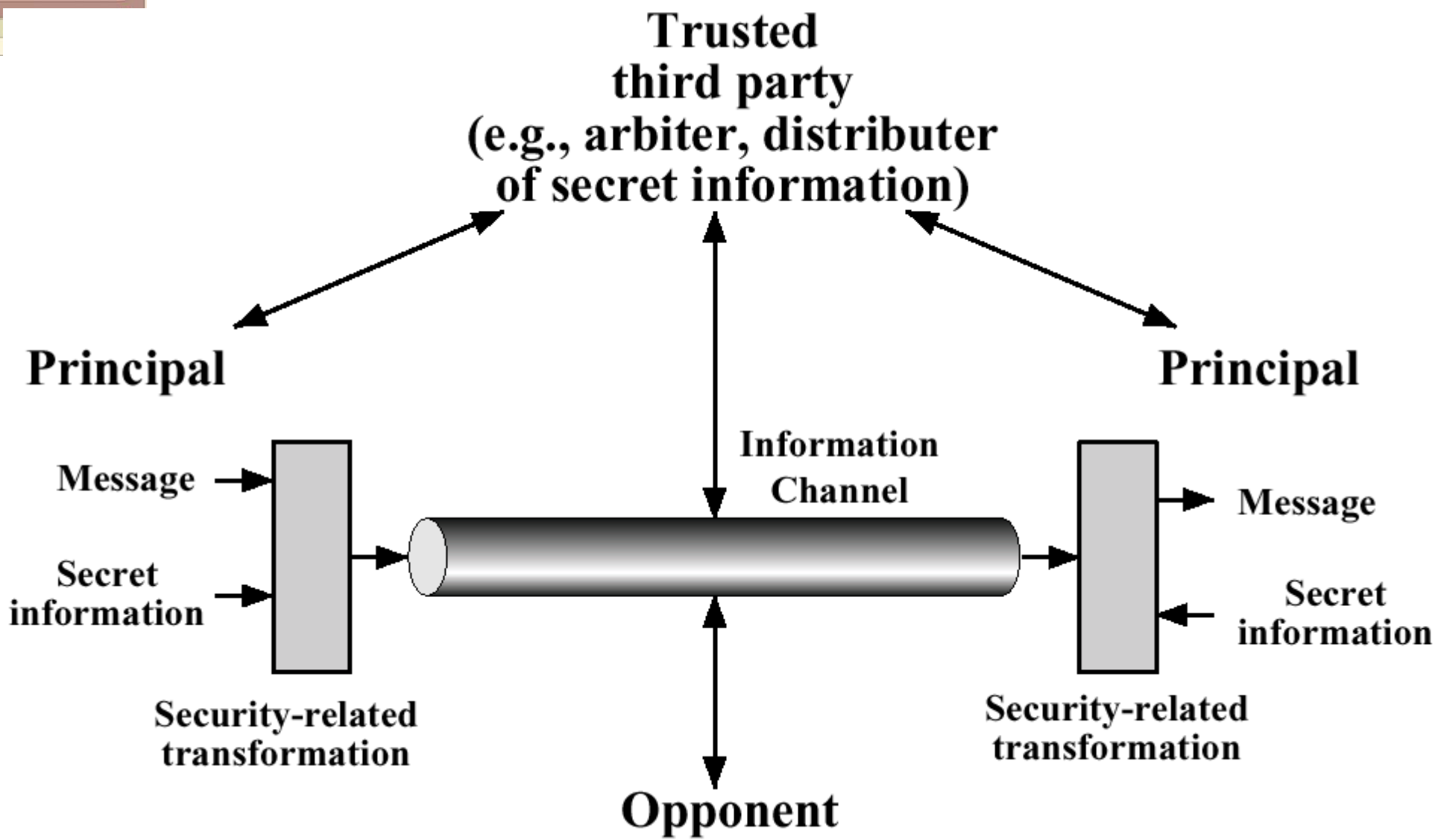
Ikke-fornektelse (nonrepudiation)

- 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!”

Aksesskontroll

- Evnen til å begrense og kontrollere tilgang til datamaskinsystemer over kommunikasjonsforbindelser
- Brukes også internt i et system

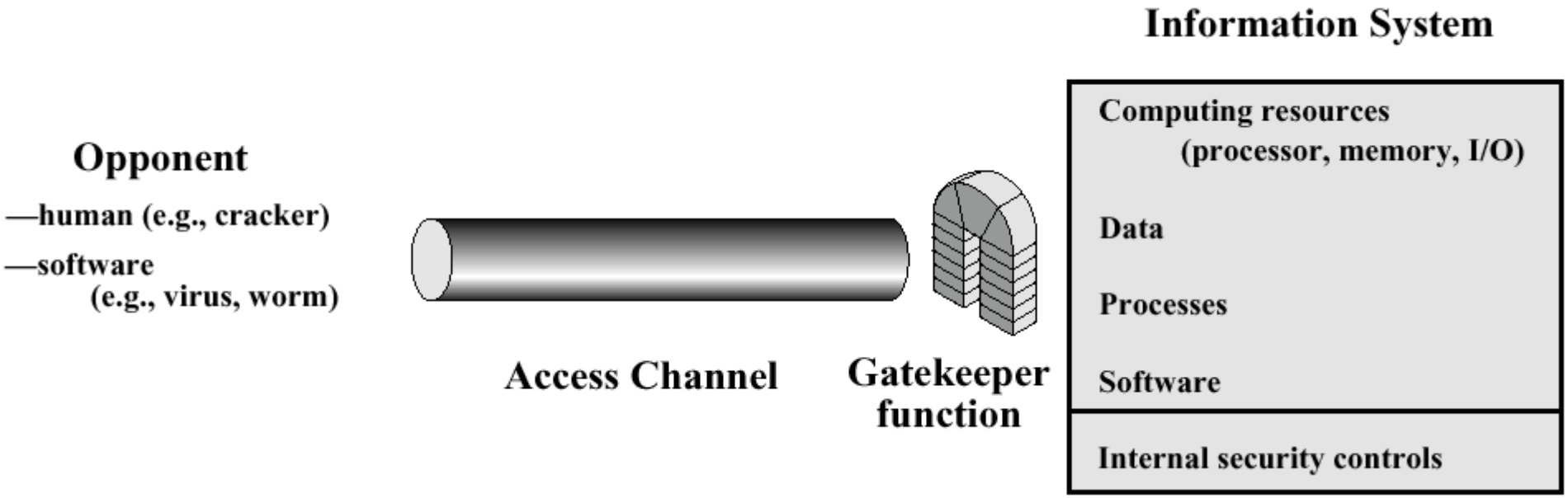
En rotete kommunikasjonsmodell



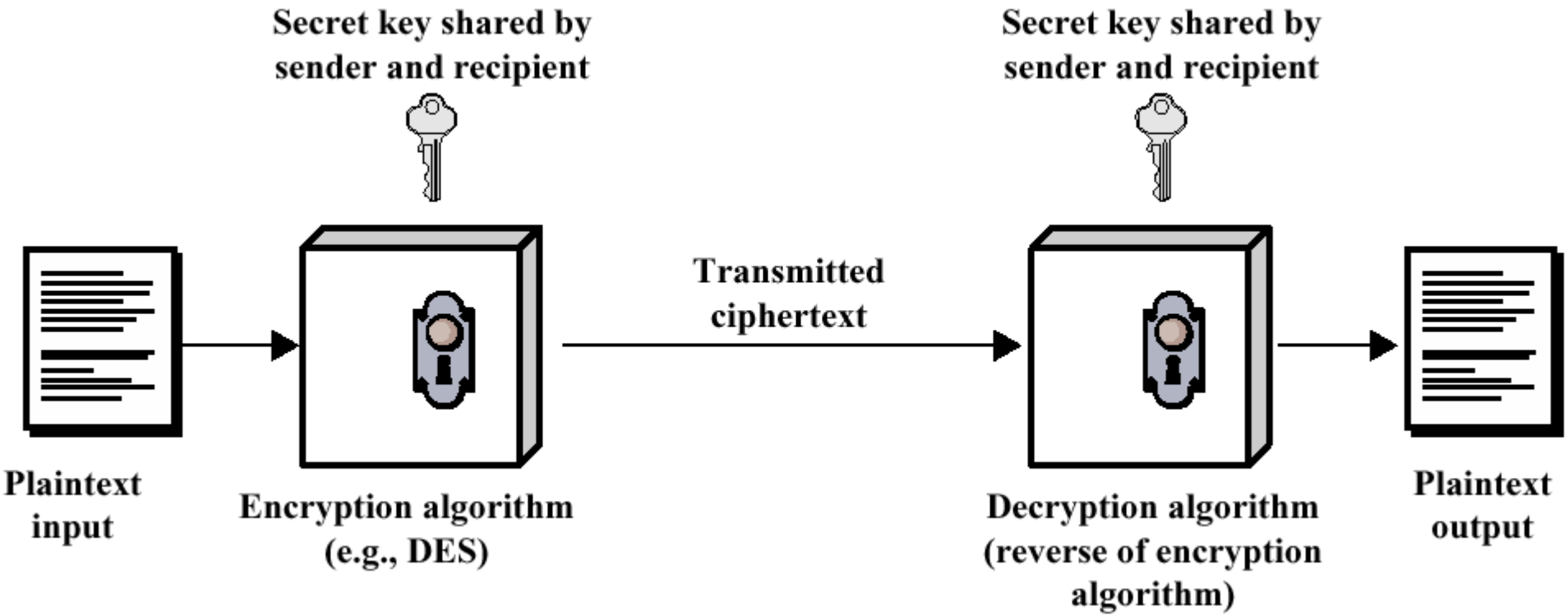
Konstruksjon av sikkerhetstjenester

- 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

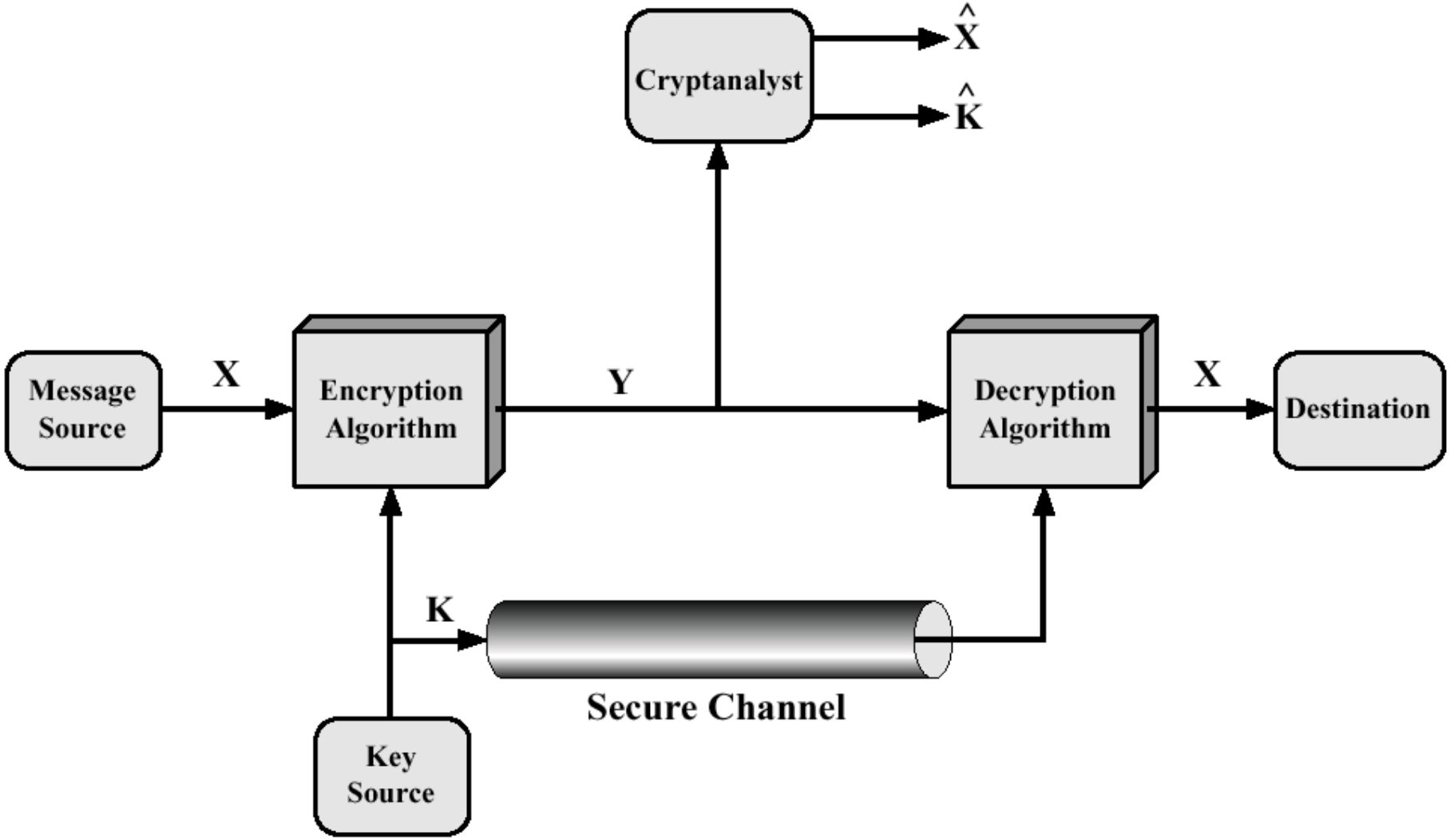
Sikkerhetsmodell for nettverksaksess



Konvensjonell kryptering



Konvensjonell krypteringsmodell



Notasjon

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

Kryptografi

Kryptografiske systemer kjennetegnes ved:

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

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”

Kryptoanalyse

- Bare-chiffertekst
- Kjent klartekst
- Valgt klartekst
- Valgt chiffertekst
  - Asymmetriske algoritmer

- Det endelige målet er vanligvis nøkkelen

Steganografi

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

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

Substitusjons-chiffer

- Cæsar
- Monoalfabetisk substitusjon
- Polyalfabetisk substitusjon - Vigenère

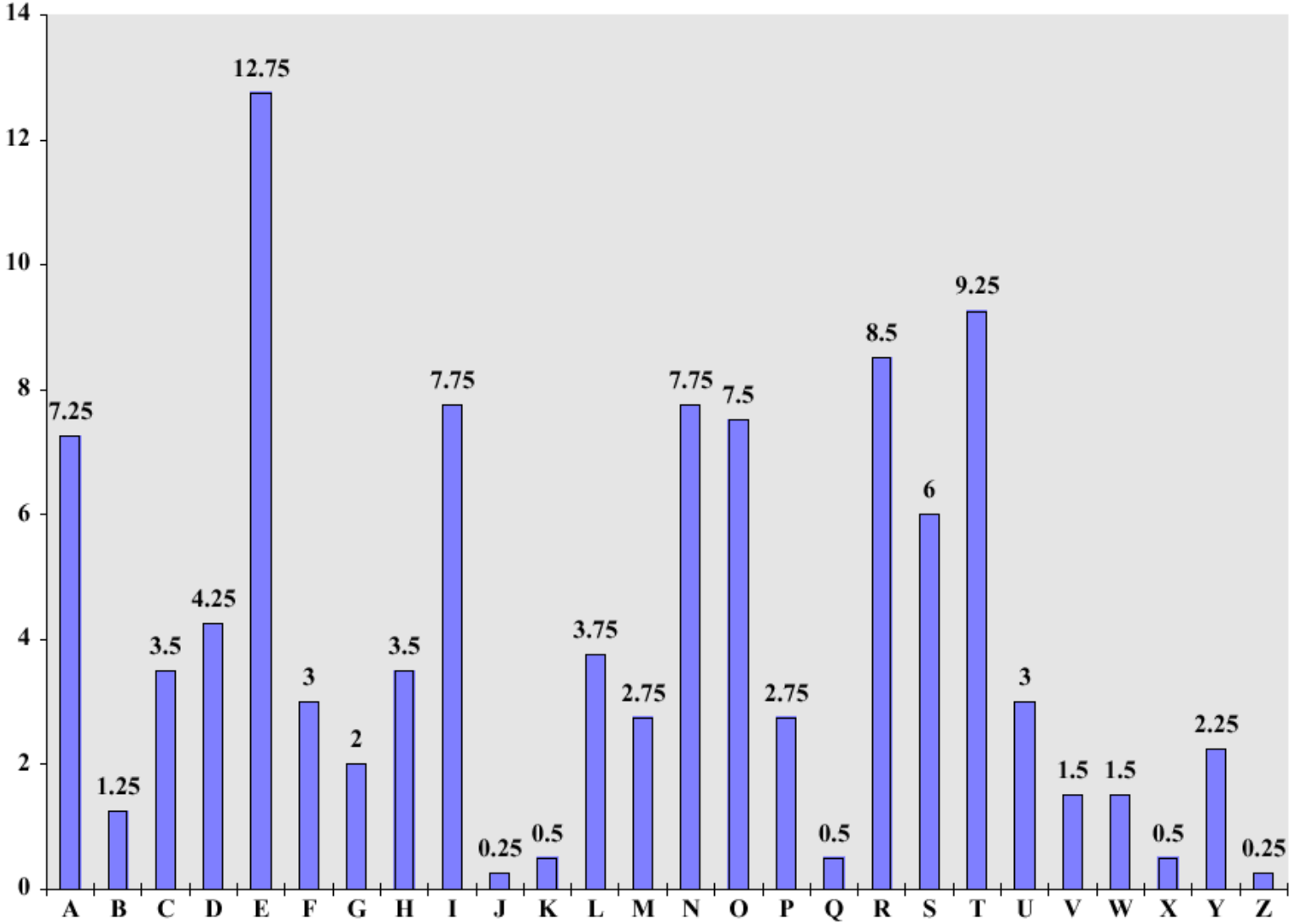
Cæsar

- 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

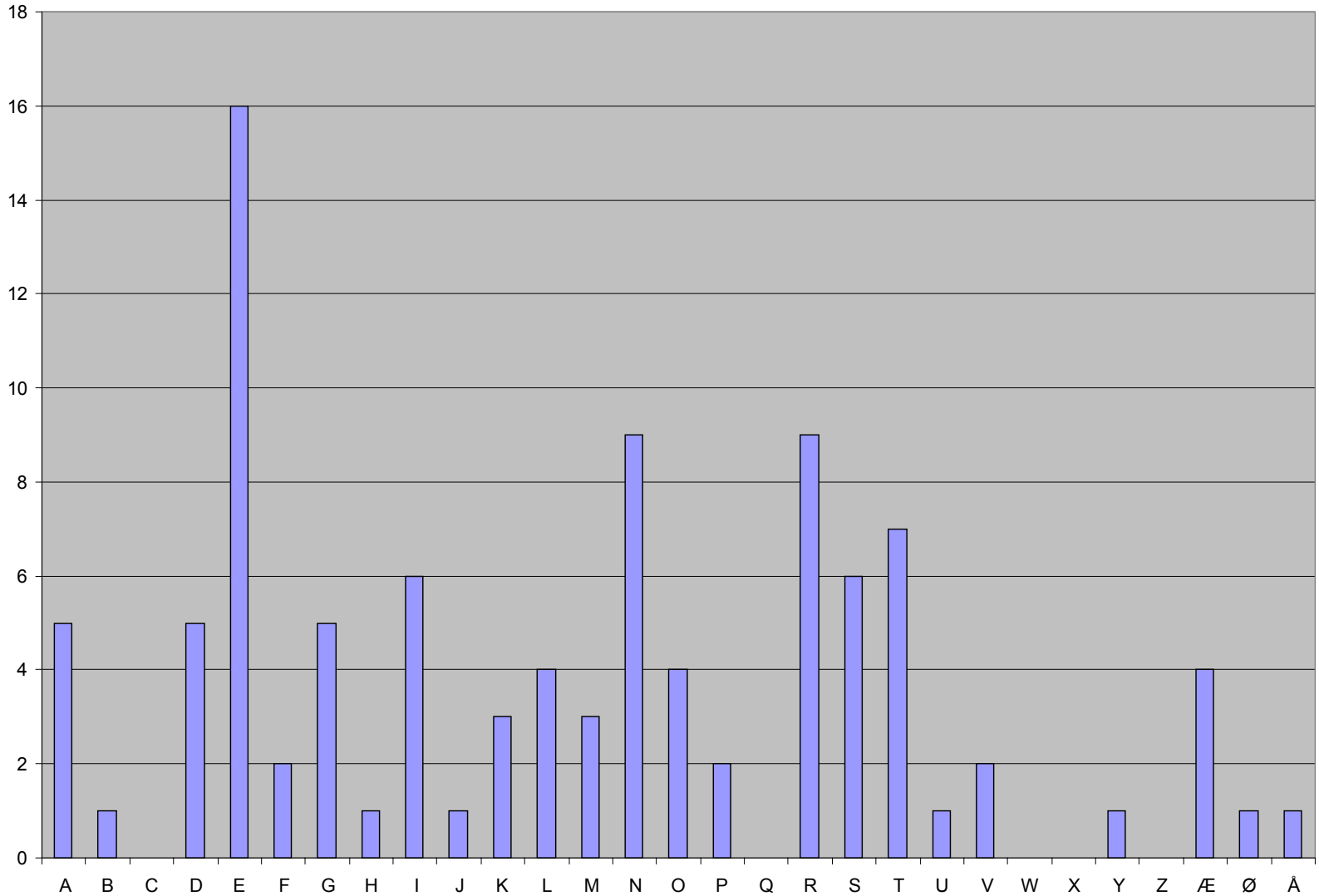
Monoalfabetisk substitusjon

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

Bokstavfordeling i engelsk tekst



Bokstavfordeling i norsk tekst



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”

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

Vigenére forts.

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

athlete

nerdnerd

One-time pad

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

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

Moderne teknikker

Moderne teknikker

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

Feistel-chiffer

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

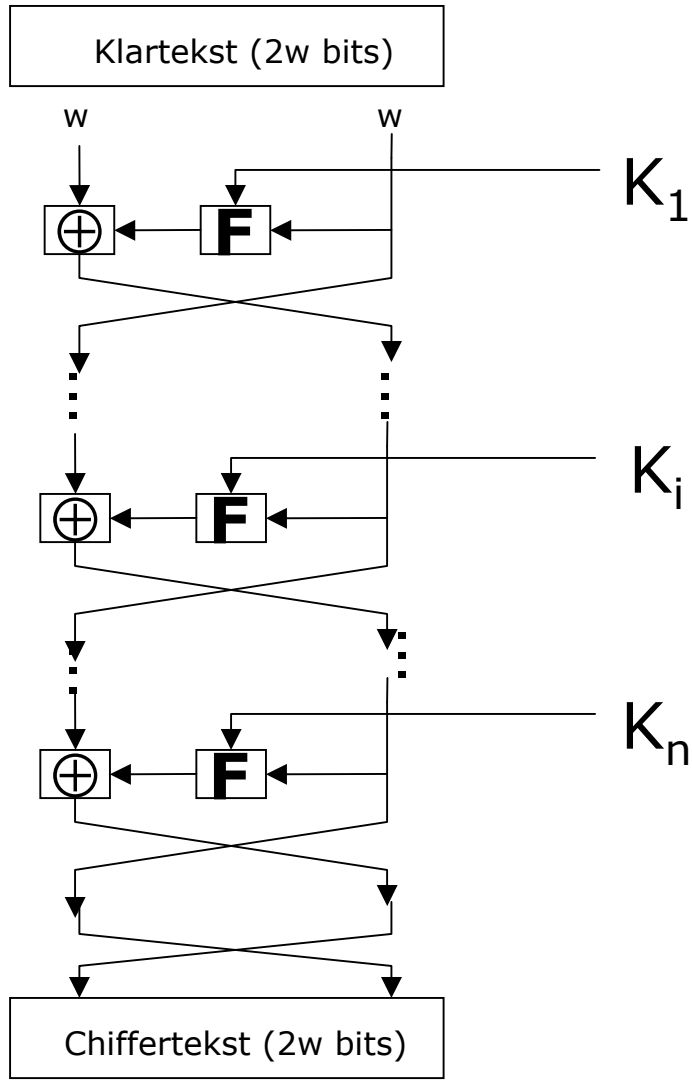
Feistel forts.

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

Avalanche-effekt

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

Klassisk (n-round) Feistel nettverk



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

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”

Moderne kryptoanalyse

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

Moderne Brute-Force

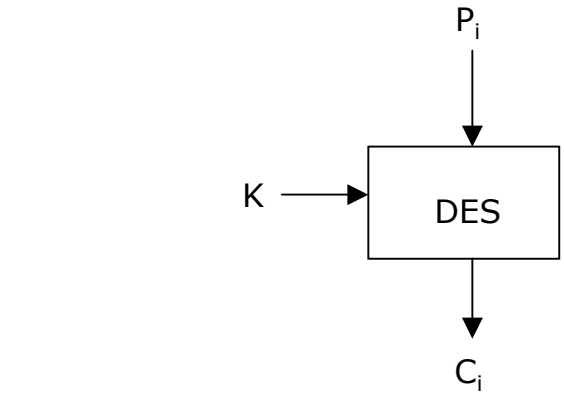
- EFF ”Deep Crack” kan knekke DES ”brute force” i løpet av noen dager
- Distributed.Net i samarbeid med EFF løste DES-III konkurransen i løpet av 22 timer

Design-kriterier

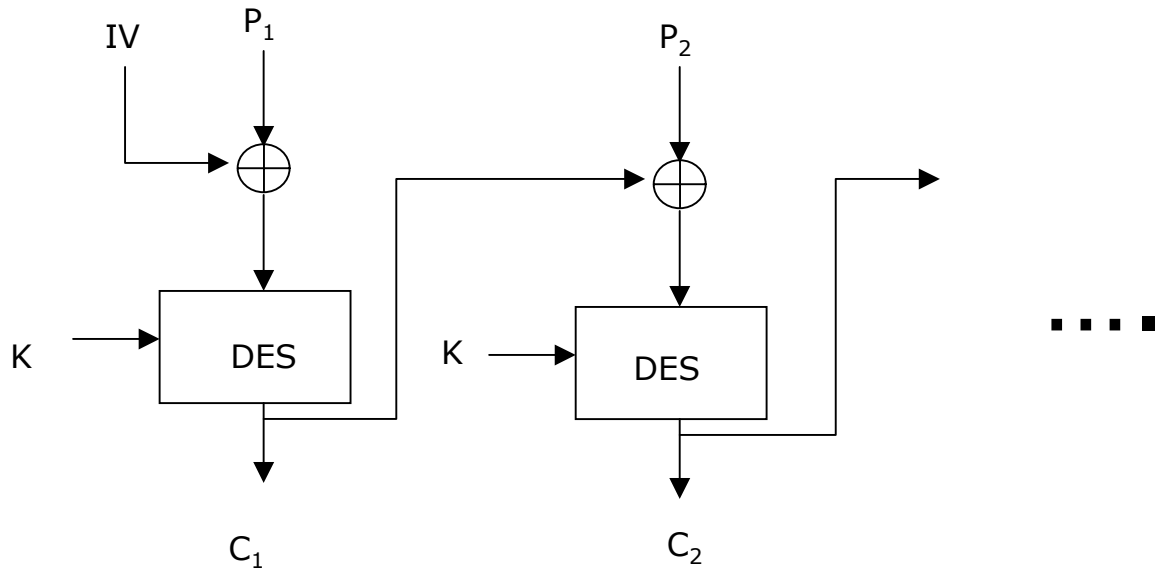
- Avalanche-effekten
- Motstandsdyktighet mot differensiell kryptoanalyse
- Antall runder
  - Gjør kryptoanalyse vanskeligere enn ”brute force”

Modi for Blokk-chiffer

ECB

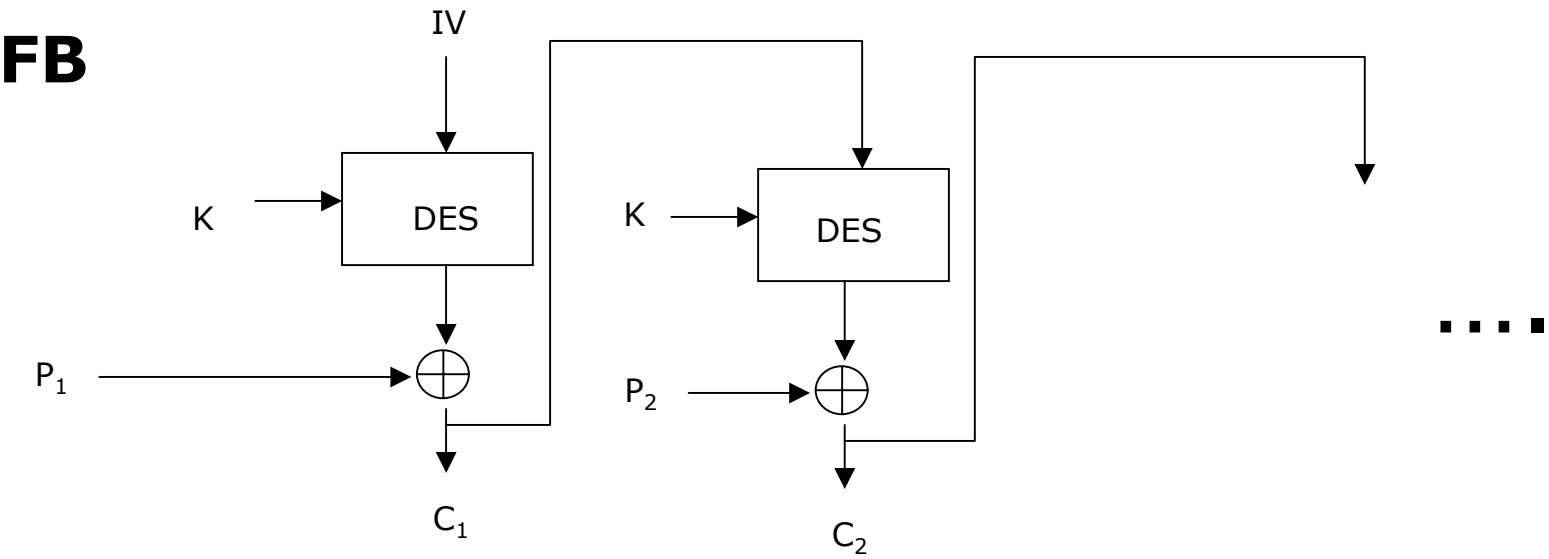


CBC

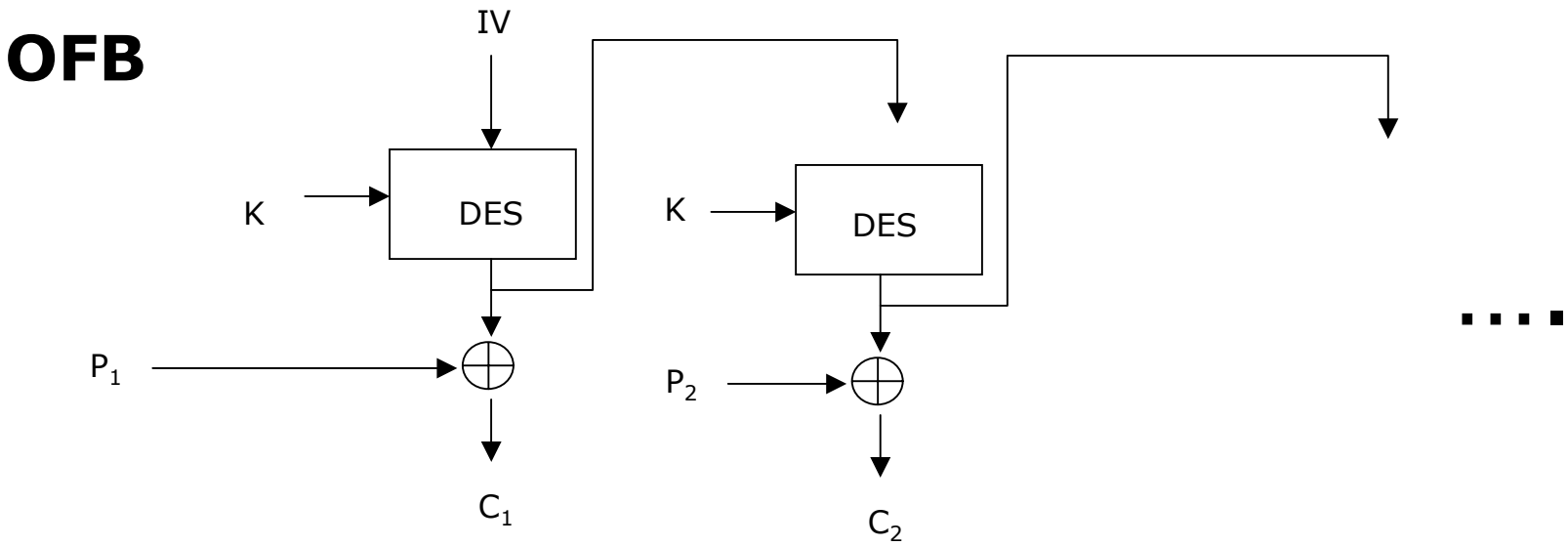


Modi, forts.

CFB



Modi, forts. forts



Dagens website

- http://www.counterpane.com