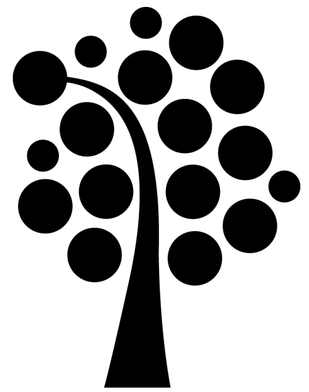
Introduktion

1DV425 Nätverkssäkerhet

Linnéuniversitetet

dagens agenda

- Viktiga begrepp och mål
- Verktyg för att upprätthålla målen
- Principer
- Grunderna i kryptering
- Åtkomstlista (ACL)
- Attacker (Läs delvis själva)

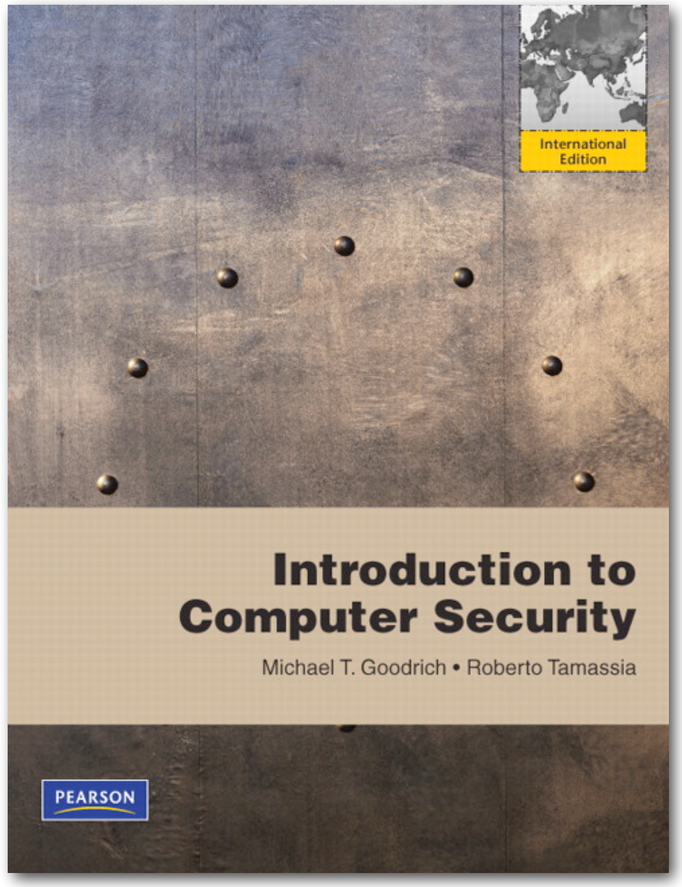


Linnéuniversitetet

Litteratur

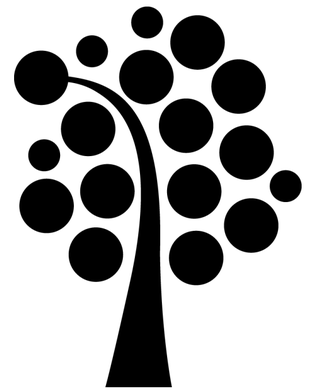
- Goodrich, T. M. & Tamassia, R. 2011. *Introduction to Computer Security*

OBS! Boken finns i olika versioner. Vi kommer använda den som heter International Edition



Säkerhet

Varför säkerhet?

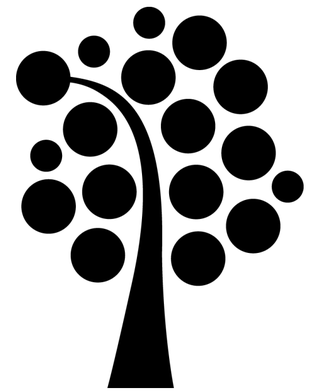


Linnéuniversitetet

Vad är det vi ska skydda?

Vad är då information ?

Det är inte formatet som styr utan värdet och känsligheten



Linnéuniversitetet

”Information är en tillgång som, liksom andra viktiga tillgångar i en organisation, har ett värde för en organisation och följaktligen måste få ett lämpligt skydd.

Informationssäkerhet syftar till att skydda information mot en mängd olika hot för att säkerställa verksamhetens kontinuitet, minska skador på verksamheten och maximera avkastningen på investerat kapital samt affärsmöjligheter”

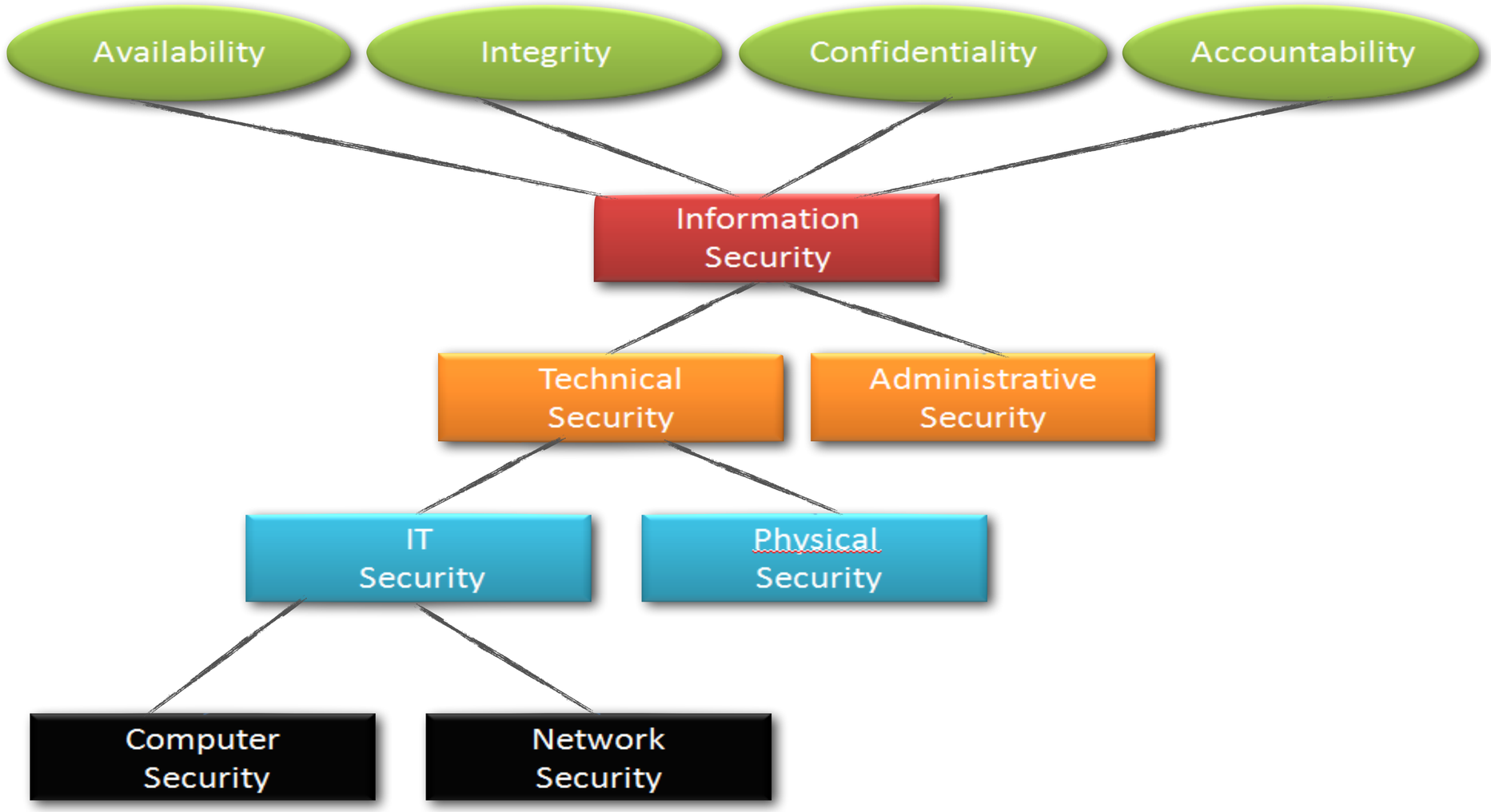
Hämtad från Svensk Standard SS-ISO/EIC 17799:2000

Linnéuniversitetet

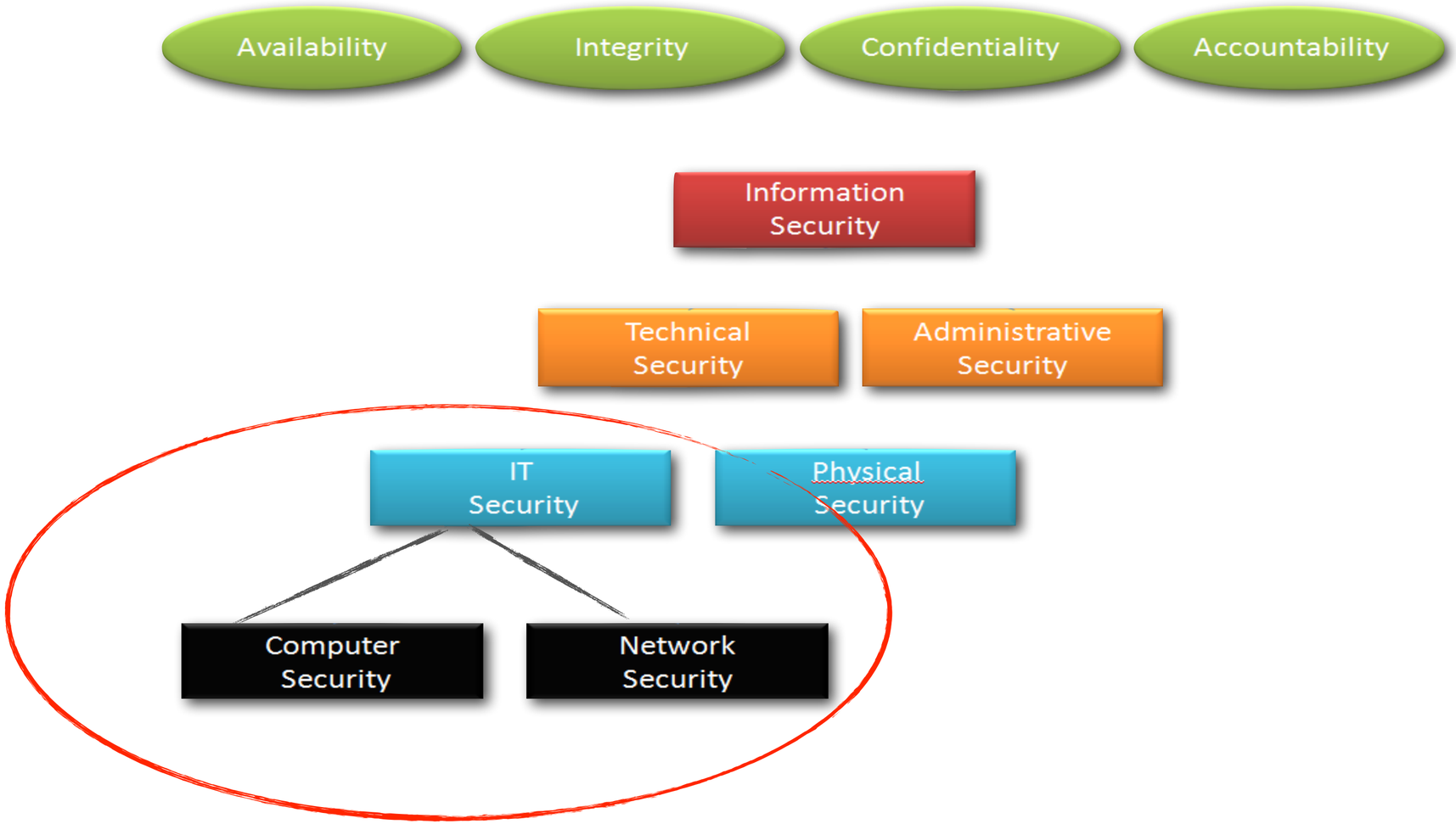
Viktiga Begrepp

- Sekretess
- Integritet (riktighet)
- Tillgänglighet
- Spårbarhet

Linnéuniversitetet



Linnéuniversitetet



IT-säkerhet är samlingsnamnet på tekniken som stödprocess för att upprätthålla/etablera informationssäkerhet…

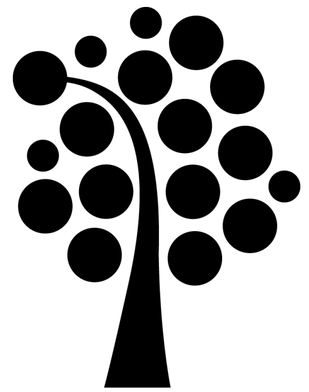
Linnéuniversitetet

Mål

Linnéuniversitetet

Konfidentialitet (Sekretess)

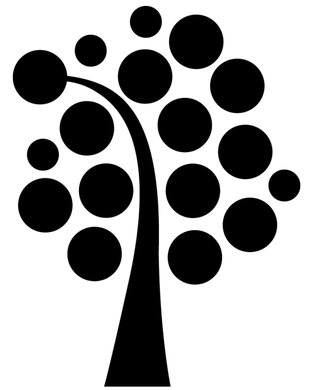
- Sekretess handlar om att undvika obehörigt röjande av information/data
- Endast behöriga användare ska ha tillgång
- Skydd av data
- Ge tillgång till de som är behöriga



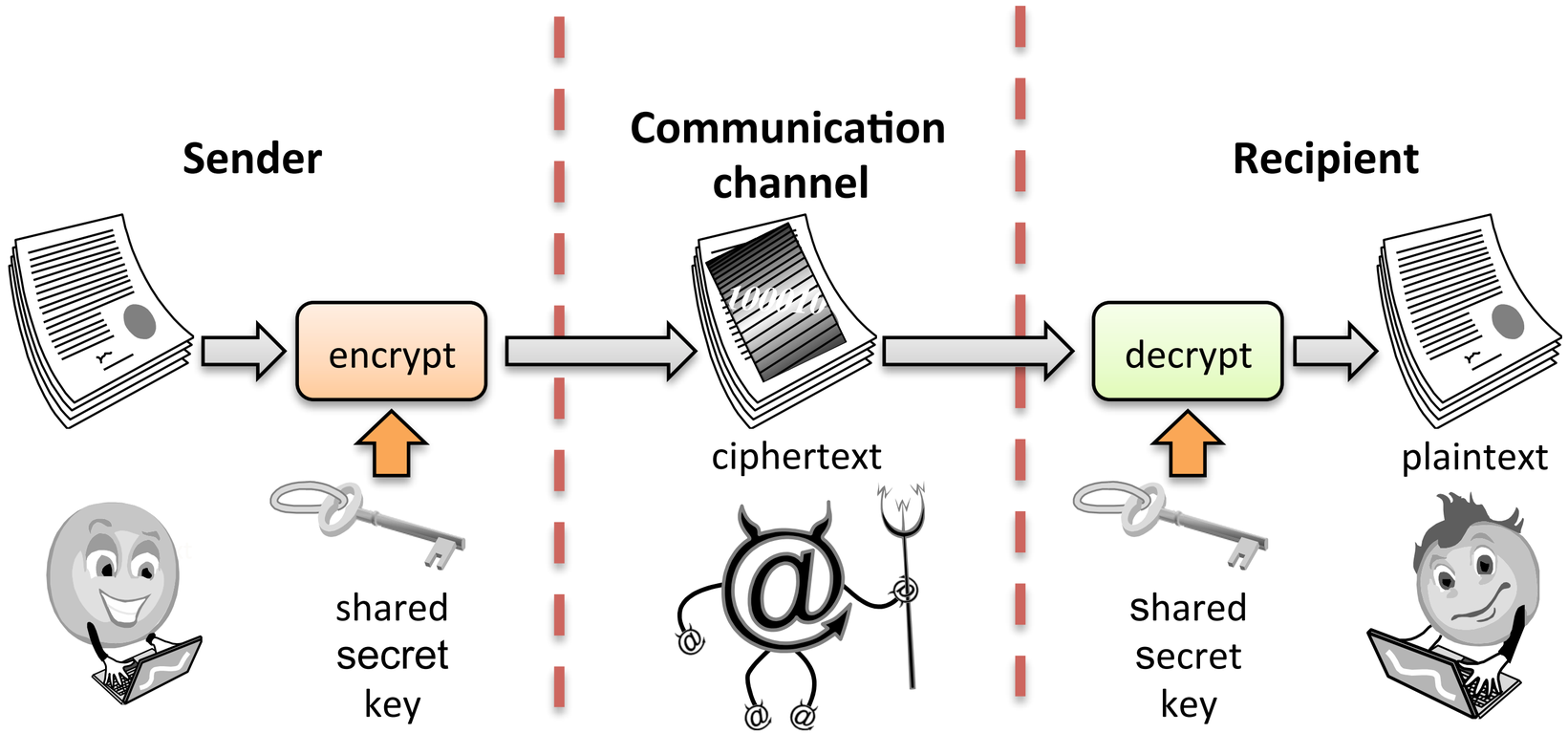
Verktyg - Sekretess

Kryptering

- Omvandla information/data genom en hemlighet
- Nyckel (kryptering/dekryptering)

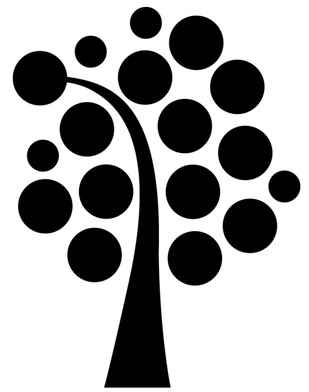


Linnéuniversitetet



Verktyg - Sekretess

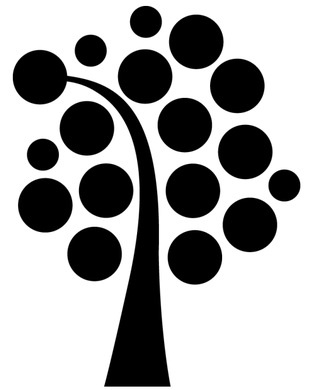
- Behörighetskontroll (Access control)
- Regler och policys som som styr tillgången till sekretessbelagd information för människor och/eller system med behov ”att veta”.
- identitet (namn, serienummer)
- roll (chef, it-tekniker)



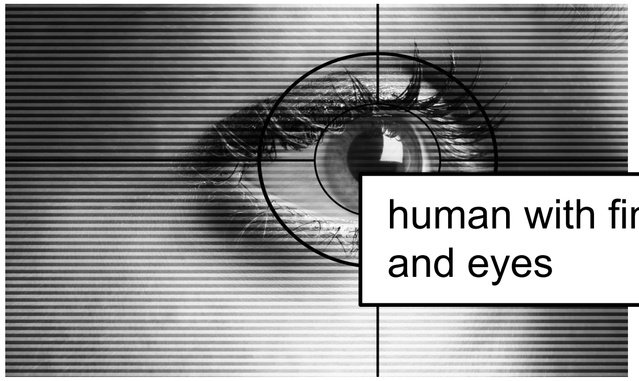
Verktyg - Sekretess

Autentisering

- Avgöra någons identitet eller roll
- Kan göras på en mängd olika sätt



Linnéuniversitetet



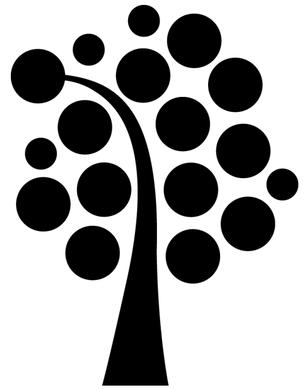
Something you are

Something you know

Something you have

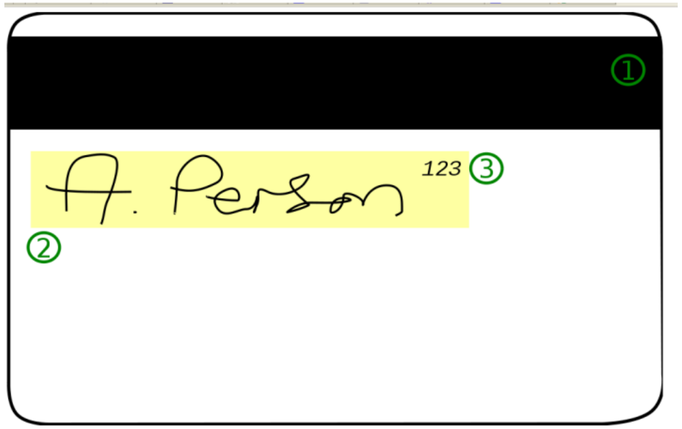
Exempel

Public domain image from http://commons.wikimedia.org/wiki/File:Bpass.jpg



Linnéuniversitetet

Exempel

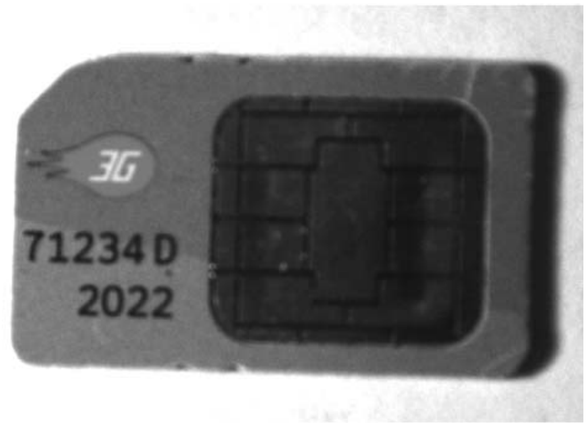


Public domain image by *Alexander Jones* from http://commons.wikimedia.org/wiki/File:CCardBack.svg

Public domain image from http://en.wikipedia.org/wiki/File:Carte_vitale_anonyme.jpg

Linnéuniversitetet

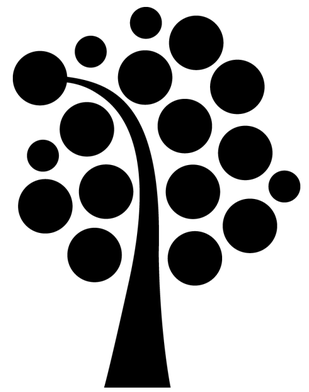
Exempel



Verktyg - Sekretess

AUKTORISATION

- Avgöra om personen eller systemet har/får tillgång till resurser
- Åtkomstpolicy (Access Control Policy)

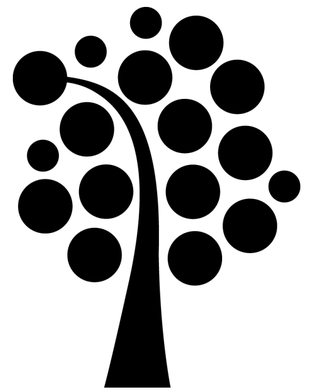


Linnéuniversitetet

Verktyg - Sekretess

FYSISK SÄKERHET

- Etablera en fysisk barriär som begränsar tillgången till skyddade datorresurser
- Lås, byggnadens konstruktion, RÖS m m

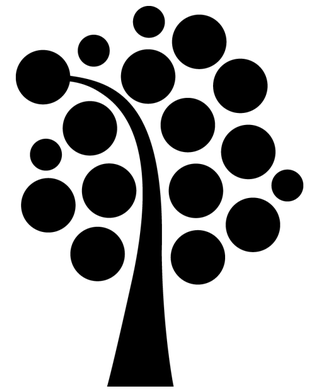


Linnéuniversitetet

Integritet

INTEGRITET

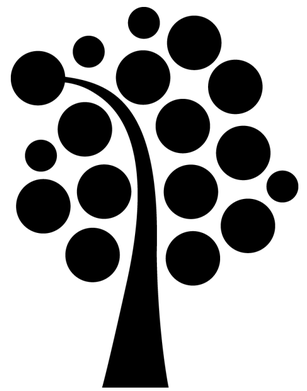
- egenskapen att information/data inte ändras på ett otillåtet sätt



Linnéuniversitetet

Verktyg - Integritet

- Backup: Schemalagd arkivering av data
- Checksummor: beräkningsfunktion som omvandlar/ översätter filens innehåll till ett numeriskt värde
- Datakorrigeringskoder: metoder för att lagra data på ett sådant sätt att små förändringar lätt kan upptäckas och korrigeras automatiskt



Tillgänglighet

TILLGÄNGLIGHET

- Egenskapen att information/data är tillgänglig för behöriga användare när behov finns

Linnéuniversitetet

Verktyg - Tillgänglighet

- Fysiskt skydd: infrastruktur som möjliggör åtkomst till information/data även om resurserna utsätts för fysisk påverkan
- Redundans: gäller såväl datorresurser som lagring

Kunde se vårdjournaler hemifrån

Vårdpersonal i Tingsryd som ville kolla schemat hemifrån upptäckte att de även kunde logga in i patienters journaler.

http://itivarden.idg.se/2.2898/1.485362/vardpersonal-ser-journaler-hemifran

Överbelastningsattacker mot svenska webbplatser

Den senaste tiden har en rad svenska myndigheters och företags webbplatser utsatts för nätattacker. MSB:s uppgift är att stödja och samordna arbetet med samhällets informationssäkerhet.

https://www.msb.se/sv/Start1/Nyheter-fran-MSB/Nyheter/Overbelastningsattacker-mot-svenska-webbplatser/

Läkare kritiska till nätjournaler

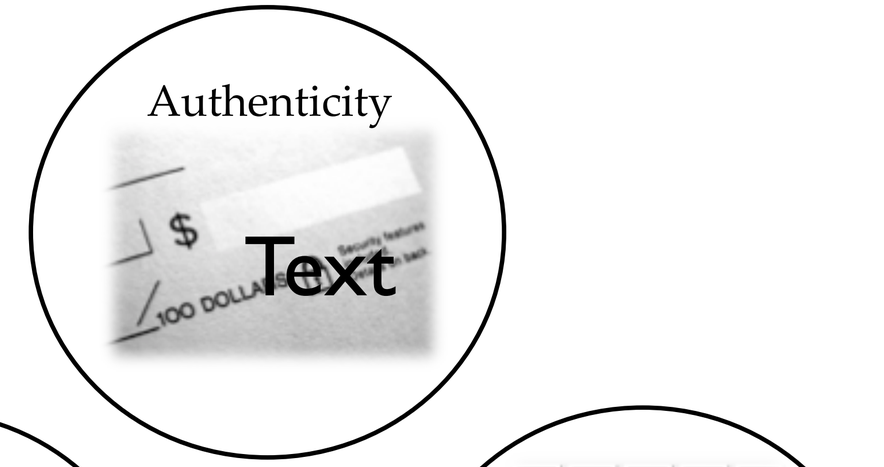
Att patienter får tillgång till sina journaler på det sätt som man planerar i Uppsala län kan strida mot gällande regler, anser Upplands allmänna läkarförening.

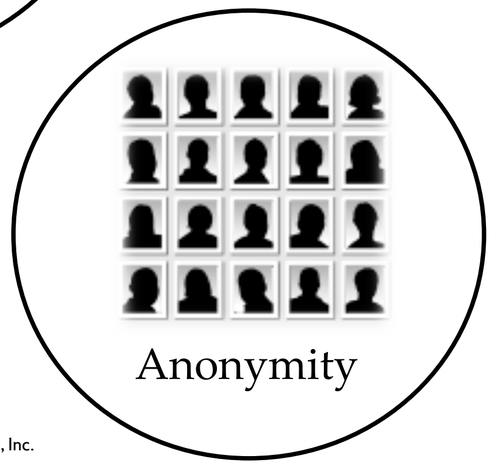
http://itivarden.idg.se/2.2898/1.459499/lakare-kritiska-till-natjournaler

Linnéuniversitetet

Andra säkerhetskoncept

A.A.A

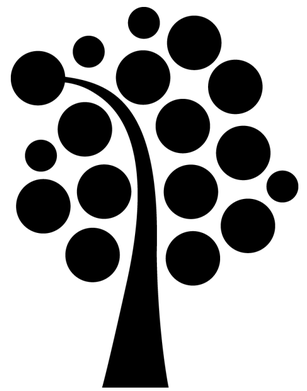




Linnéuniversitetet

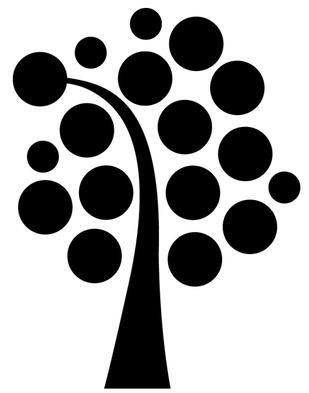
Försäkran - Assurance

- Hur tillit/förtroende (trust) erhålls och hanteras i datorsystem
- Trust management är beroende av:
  - Policies, i vilka vi specificerar beteendemässiga förväntningar dvs. hur människor och system kan och bör göra
  - Permissions, här beskrivs beteenden och handlingar som är tillåtna
  - Protections, beskriver de mekanismer som används för att vidmakthålla/tvinga permissions och policies



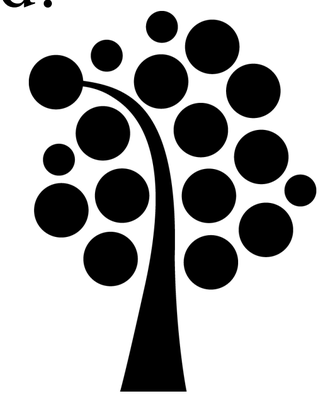
Äkthet - Authenticity

- Authenticity (äkthet): möjligheten att kunna avgöra om ett uttalande, policy och tillåtelse är äkta.
- Verktyg: digitala signaturer



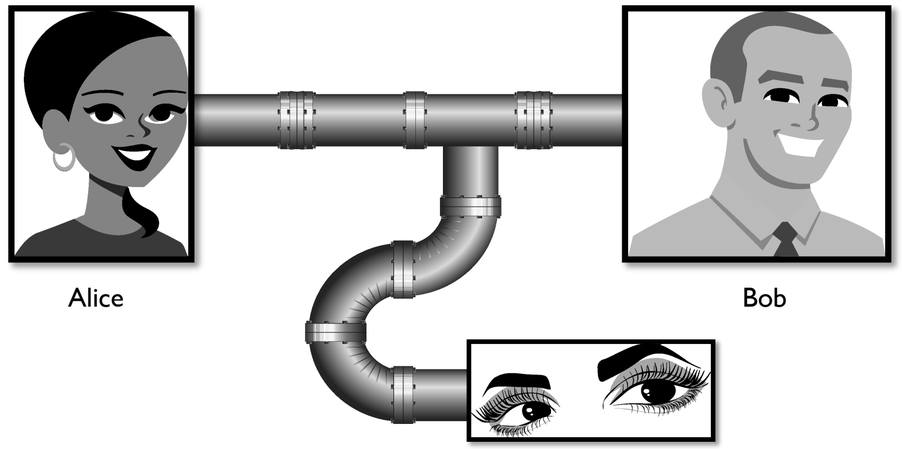
Anonymity - anonymitet

- Anonymitet: egenskapen att en viss uppgift eller transaktion inte kan härledas till en enskild individ
- Verktyg:
  - Aggregering: kombinera data från många individer på ett sådant sätt att det inte går att identifiera en enskild individ, ex. ålder eller postnummer
  - Mixing: en variant av ovanstående. Teknisk och slumpmässig metod.
  - Proxies: ”trusted agents” som hjälper individer jmf. Kina
  - Pseudonyms: uppträda under annan identitet ex. sociala medier



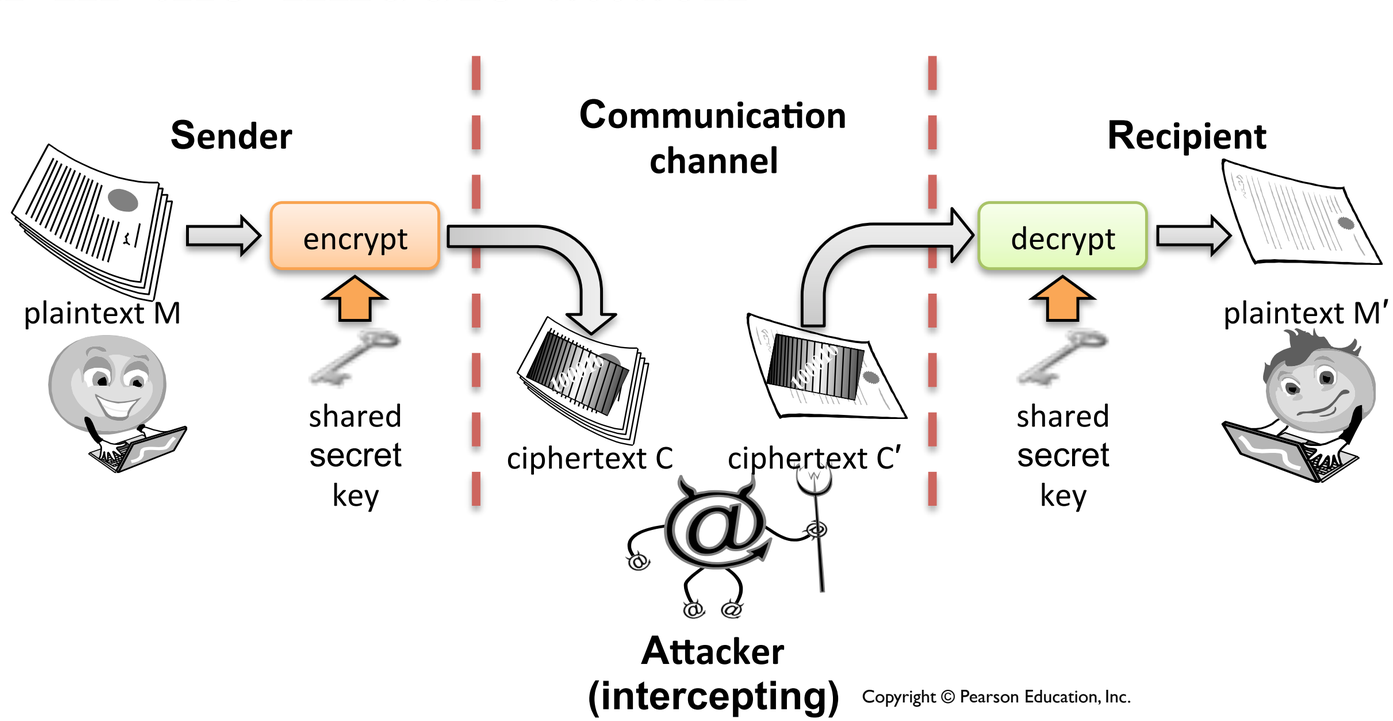
Hot & Attacker

- Avlyssning



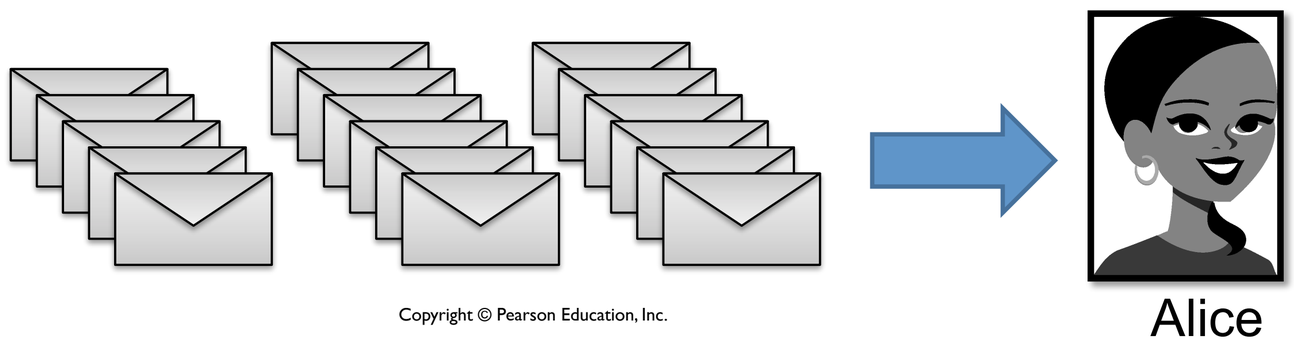
Hot & Attacker

- Förändring: obehörig förändring av information
  - Ex. Man-in-the-middle attack



Hot & Attacker

- Denial-of-service (DoS): överbelastningsattack
  - Ex. spam



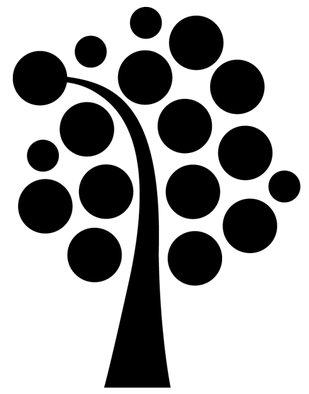
Hot & Attacker

- Masquerading: förfalska och förklä. Ex. spoofing och phishing

“From: Alice”
(really is from Eve)

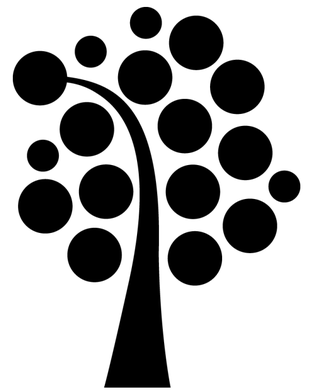
Säkerhetsprinciper

- Boken refererar till en artikel från 1975.
- J. H. Saltzer and M. D. Schroeder. The protection of information in computer systems. Proceedings of the IEEE, 63(9):1278-1308, 1975.
- 10 principer som håller än idag



1. Economy of mechanism

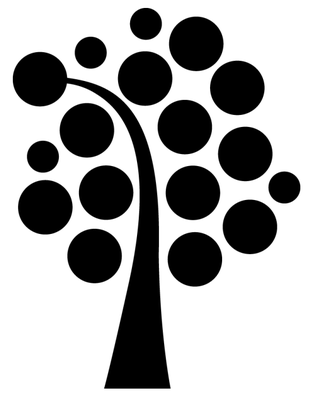
- Denna princip betonar enkelhet i såväl design och implementation av säkerhetsåtgärder



Linnéuniversitetet

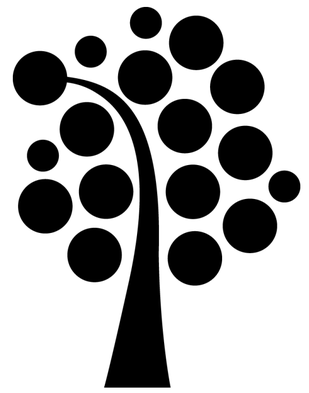
2. Fail-safe defaults

- Denna princip behandlar standardkonfiguration av system och förespråkar konservativa säkerhetsinställningar.
  - Exempelvis nya användare ska ha minimala rättigheter
  - Balans mellan säkerhet och användarvänlighet



3. Complete mediation

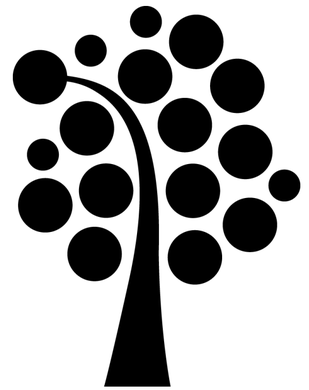
- Tillstånd/behörighet kan variera över tid.
  Behörighetskontroller bör sparas och kontrolleras igen.
- Ex. ”internet-bank”.



Linnéuniversitetet

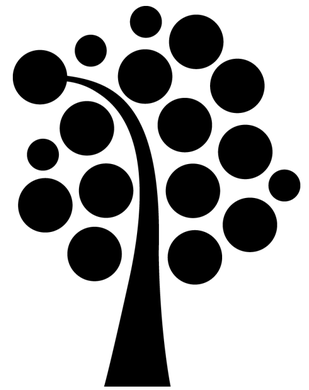
4. Open design

- Enligt denna princip bör både säkerhetsarkitektur och systemdesign vara publikt tillgänglig.
  - Kryptonycklar ska hållas hemliga men algoritmer (krypteringsalgoritmer) öppna.
  - open-source



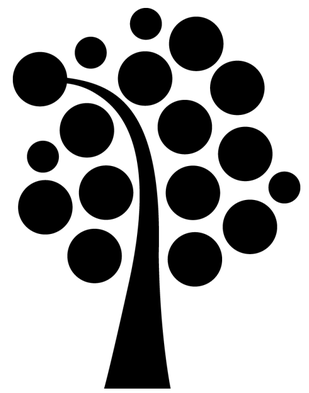
5. Separation of privilege

- Denna princip förespråkar att flera villkor/tillstånd måste uppfyllas för åtkomst till skyddade resurser.
  - har, vet
- Separation of the components; för att begränsa skadeverkan



6. Least privilege

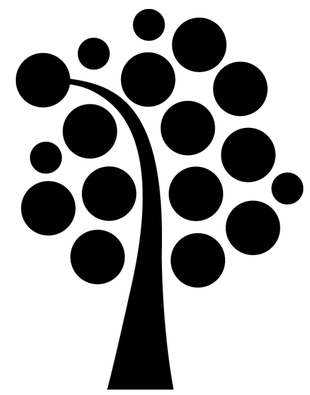
- Varje program och användare i ett system bör ha minsta möjliga rättigheter
  - jmf. militär ”inte mer information än man behöver”



Linnéuniversitetet

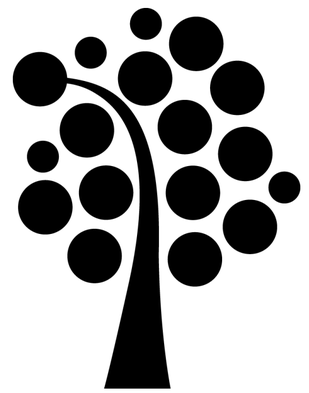
7. Least common mechanism

- I system som har flera användare (!?) så ska mekanismer som tillåter att resurser delas minimeras.
  - Ex. filer och program



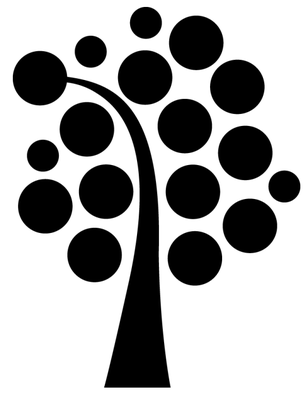
8. Psychological acceptability

- Användargränssnitt ska intuitiva (självförklarande)
- Säkerhetsrelaterade inställningar måste motsvara användarens förväntningar
  - jmf. e-postklienter och kryptering



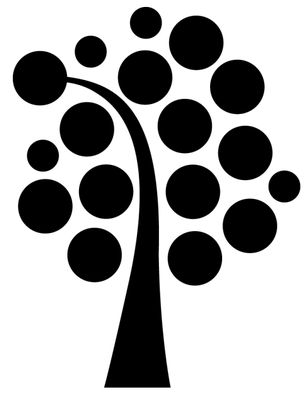
9. Work factor

- Enligt denna princip så ska ”kostnaden” att kringgå en säkerhetsmekanism jämföras med attackerarens resurser
  - jmf. Ladok och skydd av militära hemligheter



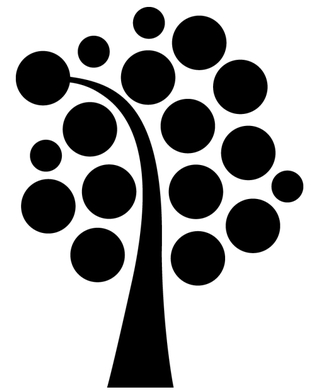
10. Compromise recordning

- Enligt denna princip kan det i vissa fall vara mer önskvärt att kunna ”logga” ett intrång än att införa mer sofistikerade motåtgärder som kan förhindra attacken.
  - jmf. övervakningskamera och/eller loggning och loggfiler



Access Control Models

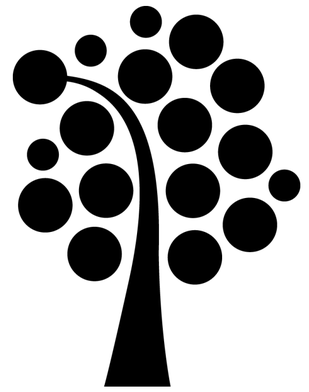
- Vem har tillgång till vad?
- Vad ska användaren kunna göra?



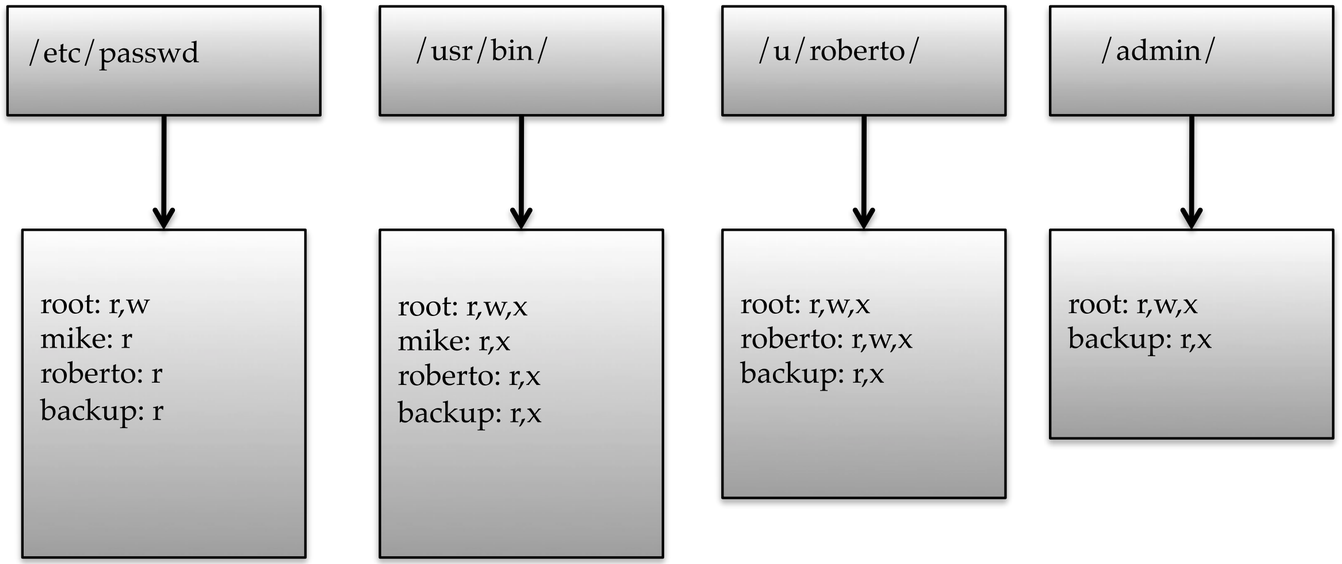
Linnéuniversitetet

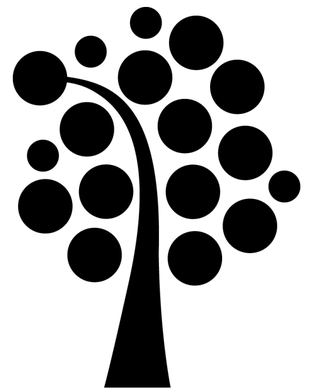
Matris (Access Control Matrix)

	/etc/passwd	/usr/bin/	/u/roberto/	/admin/
root	read, write	read, write, exec	read, write, exec	read, write, exec
mike	read	read, exec		
roberto	read	read, exec	read, write, exec	
backup	read	read, exec	read, exec	read, exec
. . .	. . .	. . .	. . .	. . .

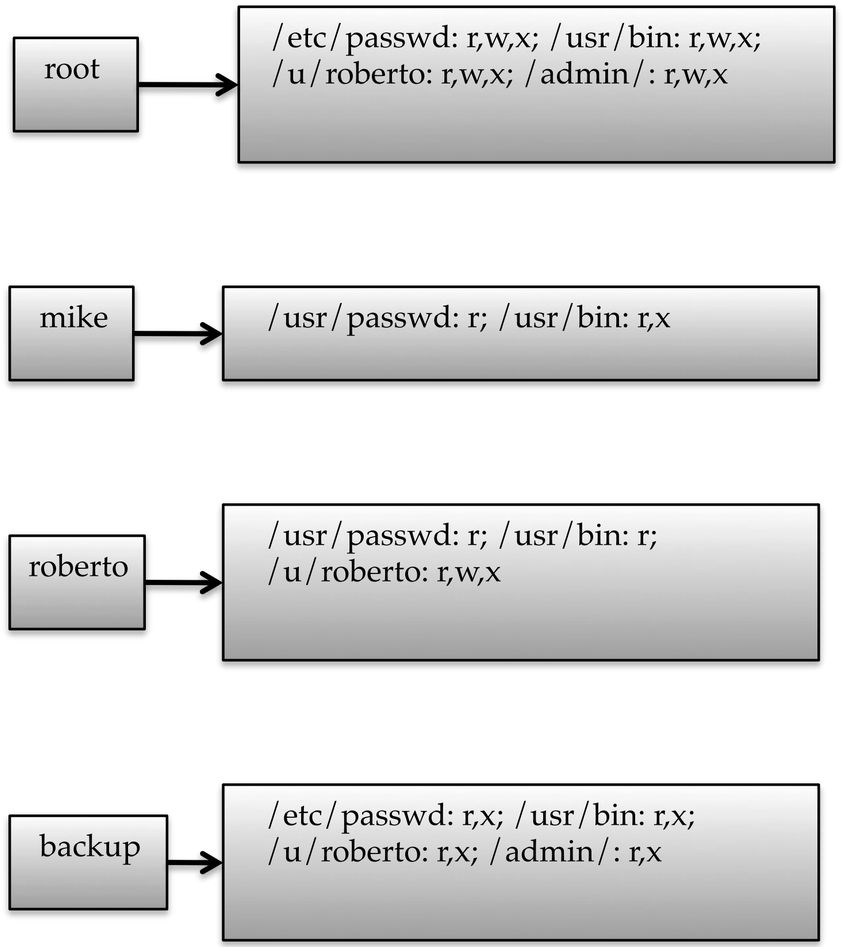


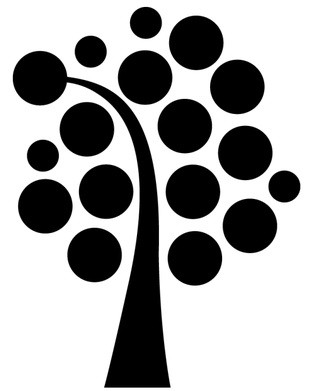
Access control lists



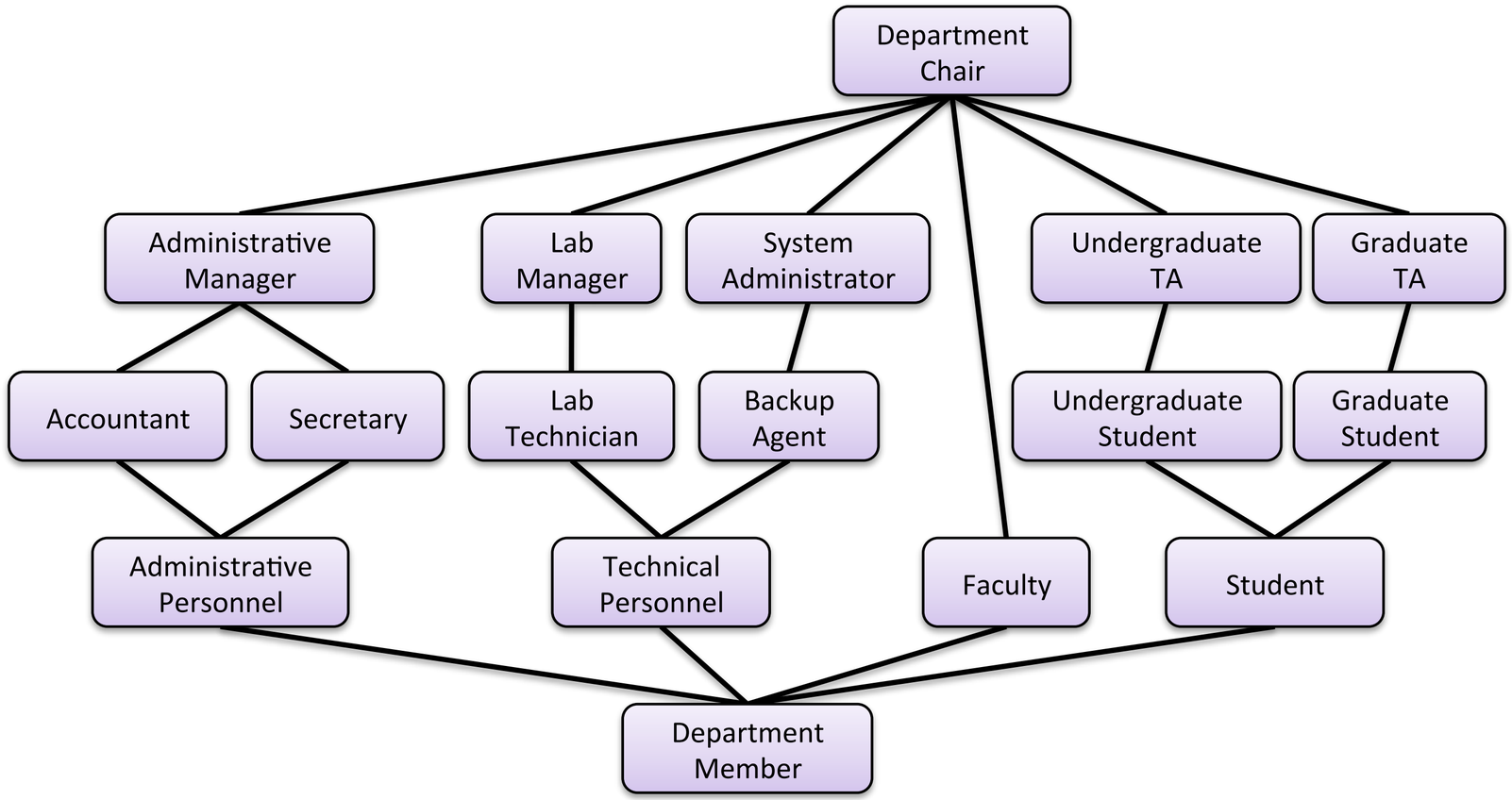


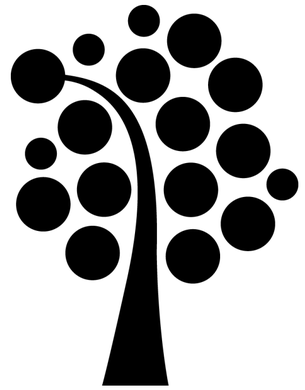
Capabilities





Role-Based Access Control

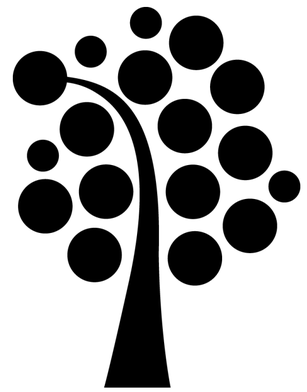




Linnéuniversitetet

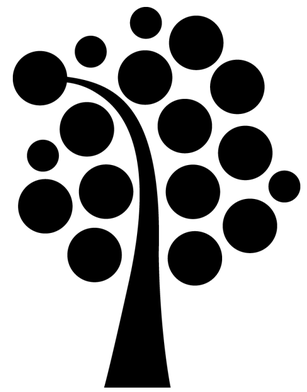
Kryptering

Linnéuniversitetet

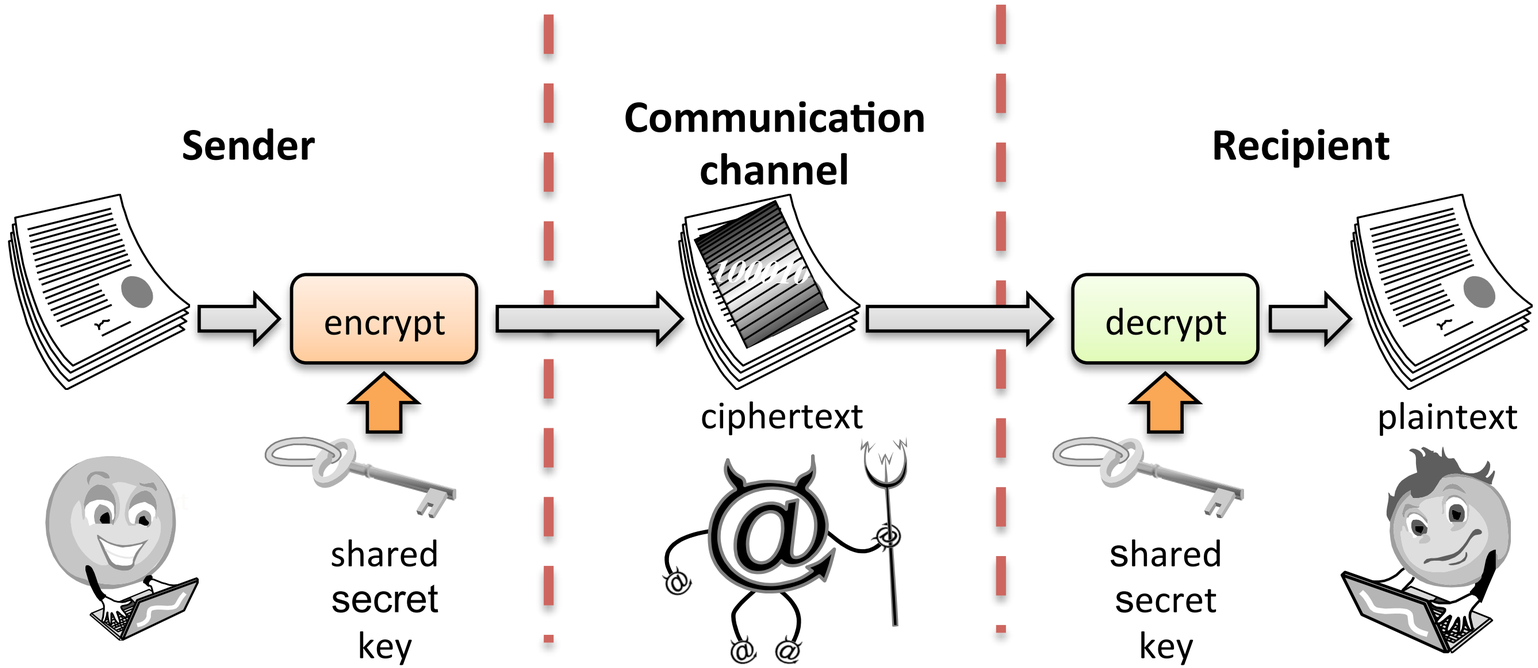


Kryptering

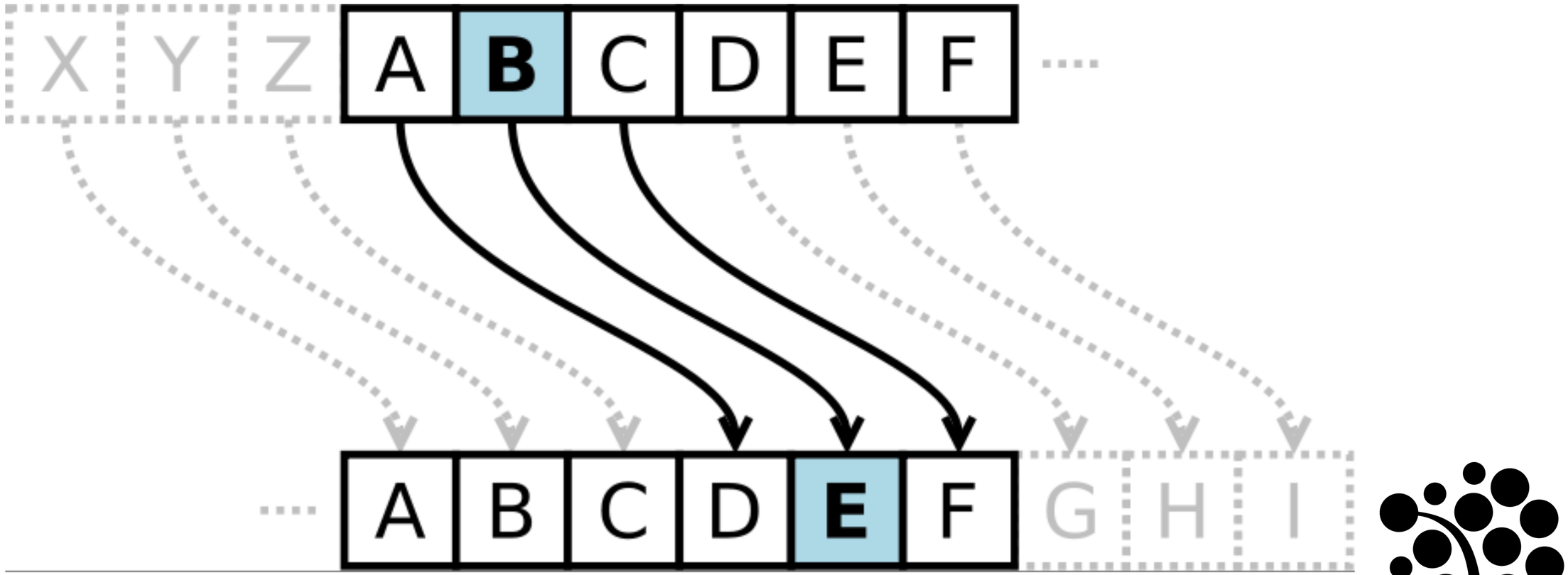
- Möjliggör säker kommunikation mellan två parter över en öppen (osäker) kommunikationskanal
- Förvränger klartexten på ett förutbestämt sätt



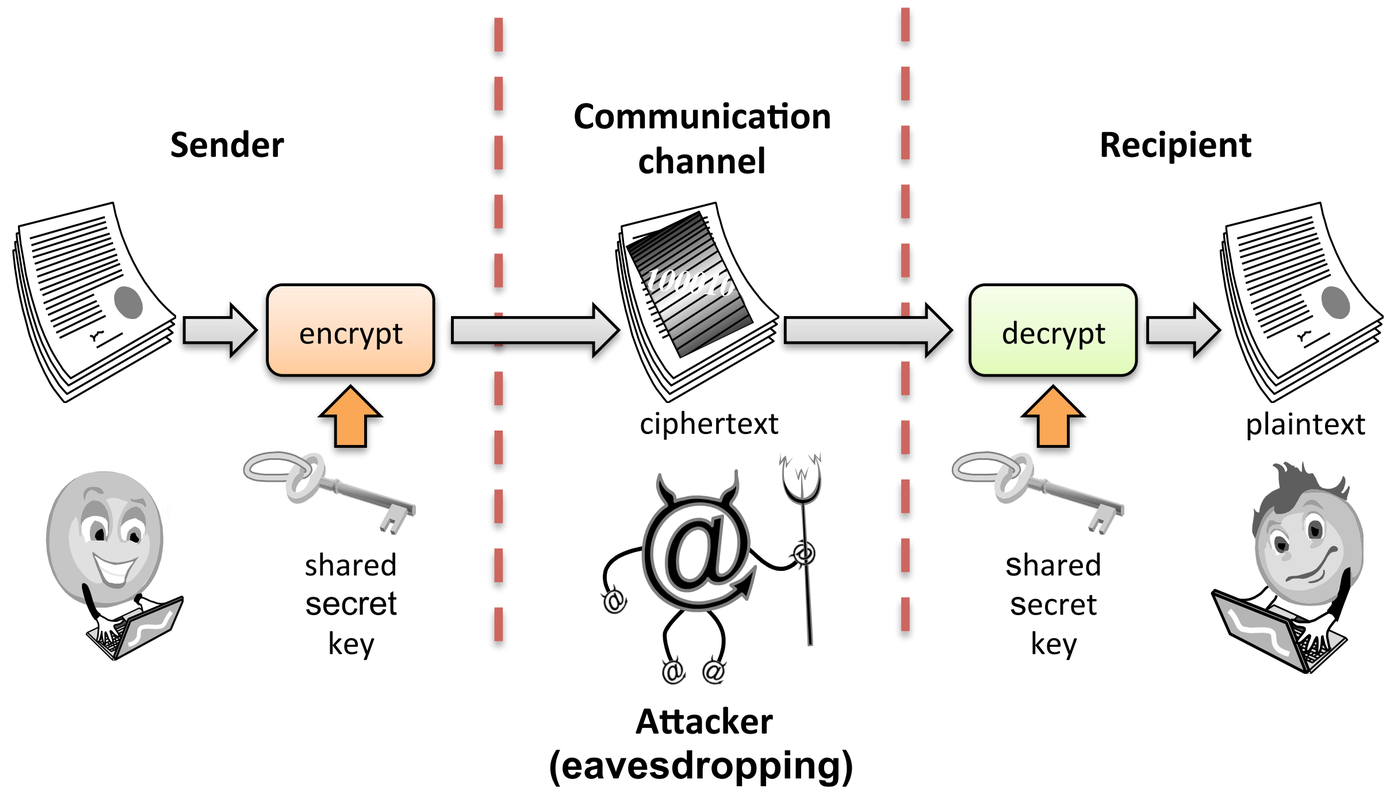
Kryptering



Caesar Cipher

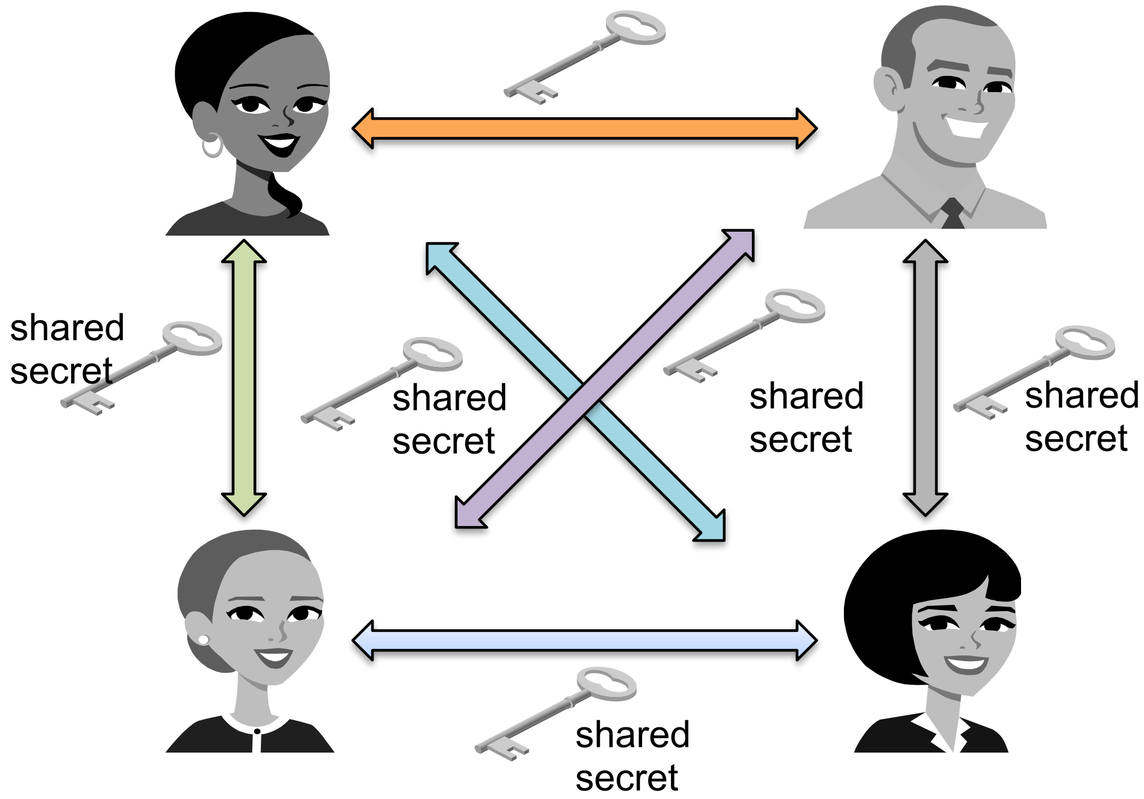


Symmetrisk kryptering



Linnéuniversitetet

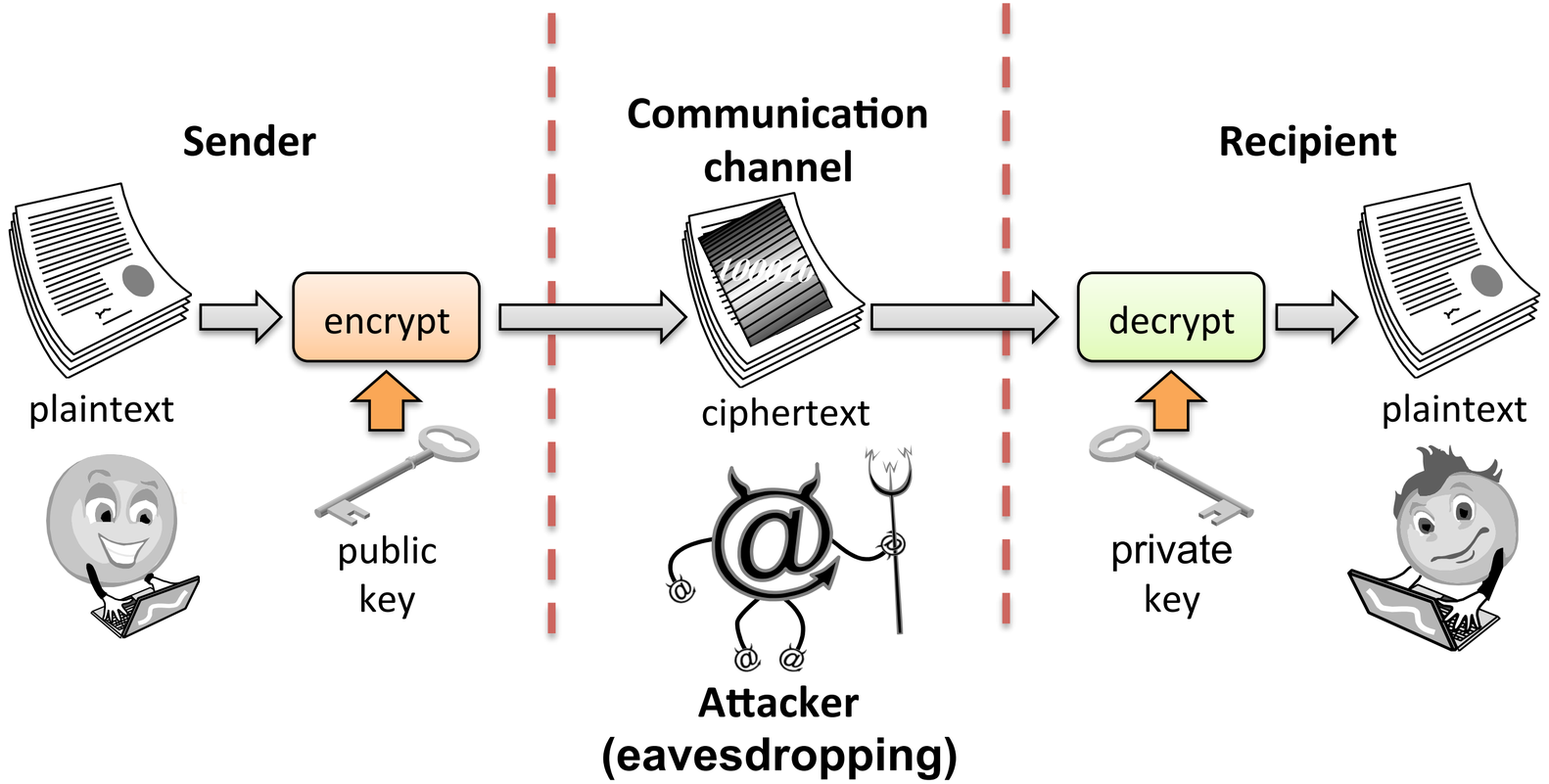
Symmetrisk kryptering

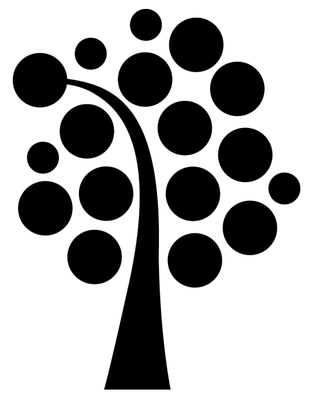


n (n−1)/2
keys

Asymmetrisk kryptering

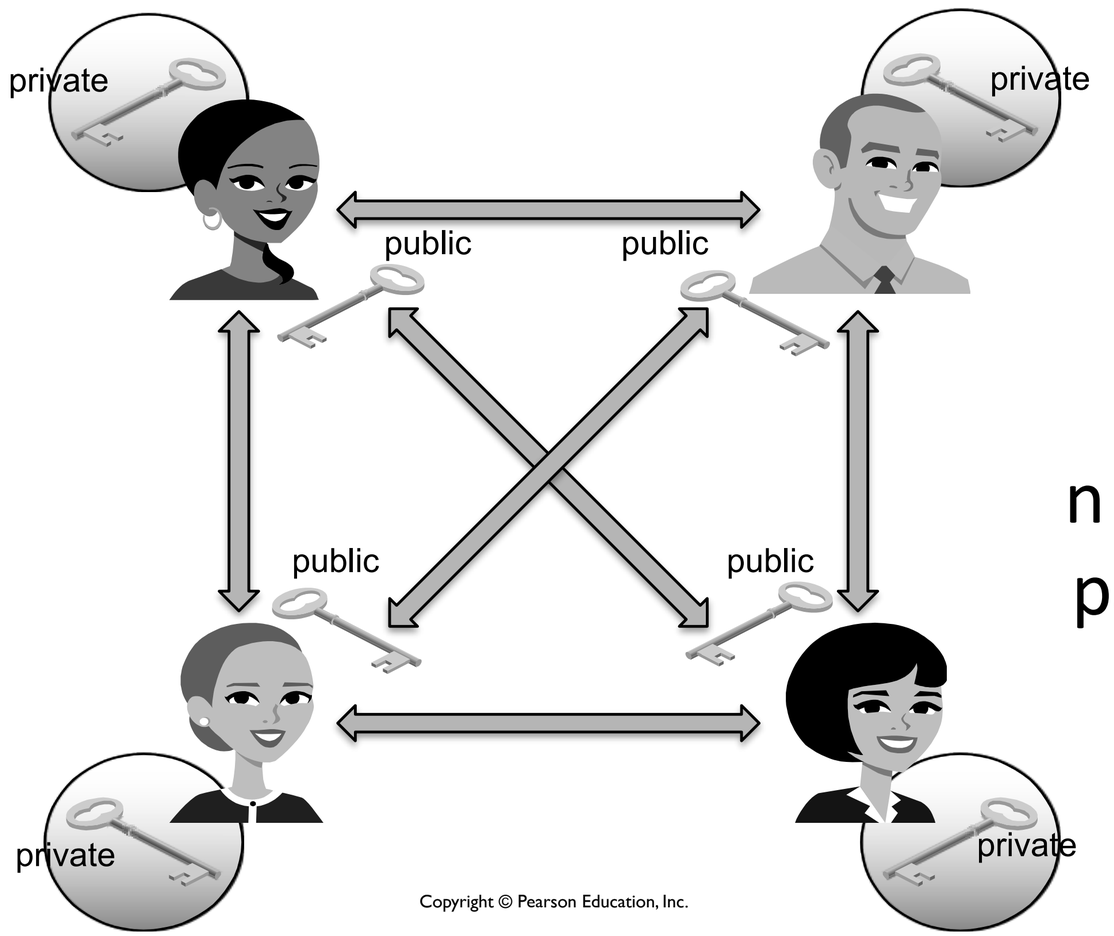
Public-Key Cryptography





Linnéuniversitetet

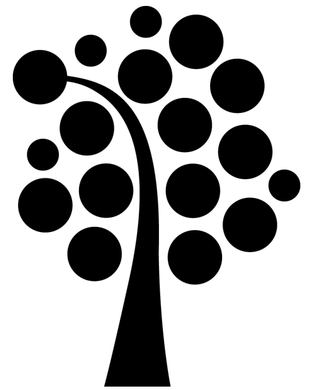
Asymmetrisk kryptering



n key pairs

Mer kryptering

- Digitala signaturer
- Hash-funktioner och checksummor
  - lösenord



Fakta om lösenord

Linnéuniversitetet

Det var allt för idag!

Linnéuniversitetet