

# El Gamal mixnät och implementering av en verifierare

## Kandidatexamensarbete - SA104X - VT2013

Erik Larsson   Carl Svensson  
Handledare: Douglas Wikström

KTH, Skolan för datavetenskap och kommunikation

# Viktigt med säkra folkomröstningar

- Röstarsäkerhet
- Verifierbarhet
- Robusthet
- Kan vi effektivisera?
  - Elektronisk röstning

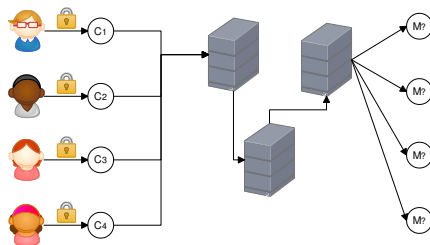


# Innehåll

- 1 Inledning
- 2 Introduktion till mixnät
- 3 Kryptografi
- 4 Mixnät
- 5 Verificatum
- 6 Implementation
- 7 Resultat
- 8 Avslut

# Mixnät - En digital tombola

- Indata:
  - Krypterade röster
- Körning:
  - Blandas hemligt
- Utdata:
  - Dekrypterade röster

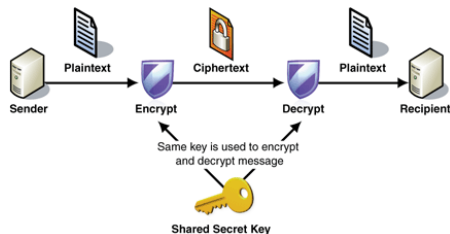


# Innehåll

- 1 Inledning
- 2 Introduktion till mixnät
- 3 Kryptografi**
- 4 Mixnät
- 5 Verificatum
- 6 Implementation
- 7 Resultat
- 8 Avslut

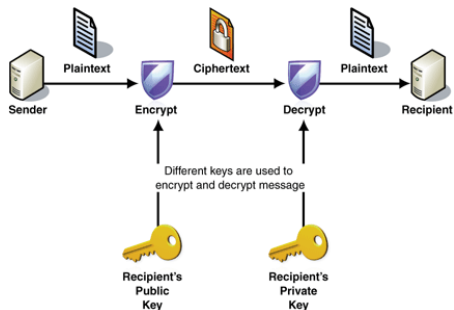
# Kryptografi

- Historia
- Symmetrisk kryptering
  - Gemensam nyckel
- Exempel
  - Caesar
  - Enigma



# Public Key Cryptography

- Räddningen
- Diffie & Hellman
- Olika nycklar
- Okända parter kan kommunicera



# El Gamal kryptografi

- Givet  $y$ ,  $g$  &  $p$ , vad är  $x$ ?
- Diskreta logaritmen svår
- Grunden i El Gamal-krypto

$$y := g^x \mod p$$

$$y := g^x \quad s \in \mathcal{R}$$

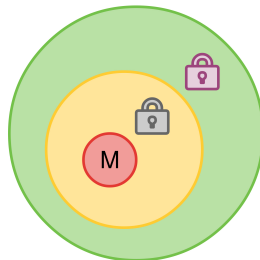
$$c = (g^s, y^s \cdot m) = (u, v)$$

$$m = u^{-x} \cdot v$$



# Egenskaper hos El Gamal

- Homomorft
  - Möjliggör flera lager kryptering
- Generalisering till andra grupper



# Zero-knowledge proof

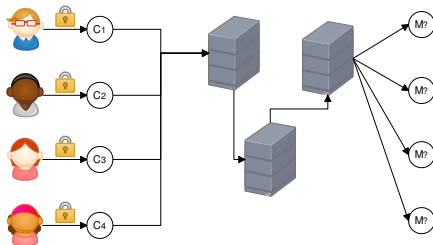
- Bevis för ett påstående
- Avslöjar inte något annat
- Exempel
  - Diskreta logaritmen

# Innehåll

- 1 Inledning
- 2 Introduktion till mixnät
- 3 Kryptografi
- 4 Mixnät**
- 5 Verificatum
- 6 Implementation
- 7 Resultat
- 8 Avslut

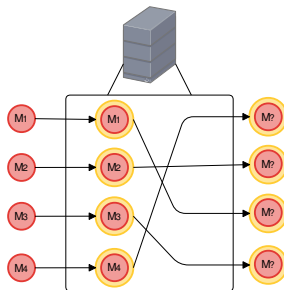
# Mixnät

- Mixnät blandar
- Hur går detta till?



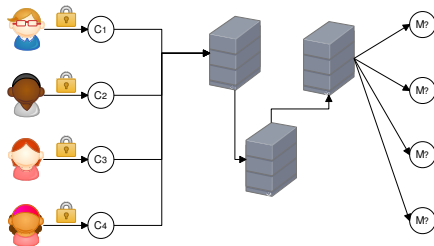
# Hur fungerar varje server?

- Indata: kryptotexter
- Kryptera om
- Blanda
- Mata ut



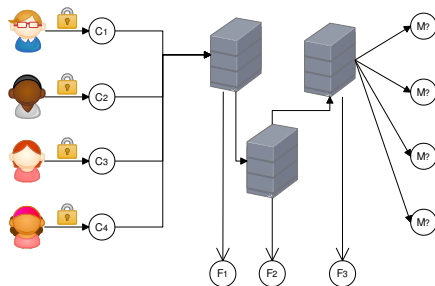
# Hur kan vi verifiera att det blir rätt?

- Verifiering
- Zero-knowledge
- Extra data

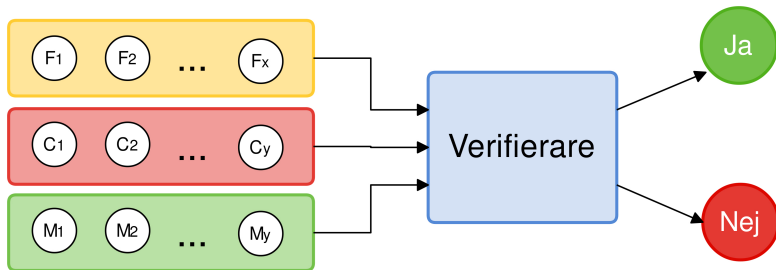


# Hur kan vi verifiera att det blir rätt?

- Verifiering
- Zero-knowledge
- Extra data



# Verifieraren analyserar körningen



- Vi får reda på om allt gått rätt till
- Fortfarande inte möjligt att veta vems röst som är vem



# Innehåll

- 1 Inledning
- 2 Introduktion till mixnät
- 3 Kryptografi
- 4 Mixnät
- 5 Verificatum**
- 6 Implementation
- 7 Resultat
- 8 Avslut

# Vad är Verificatum?

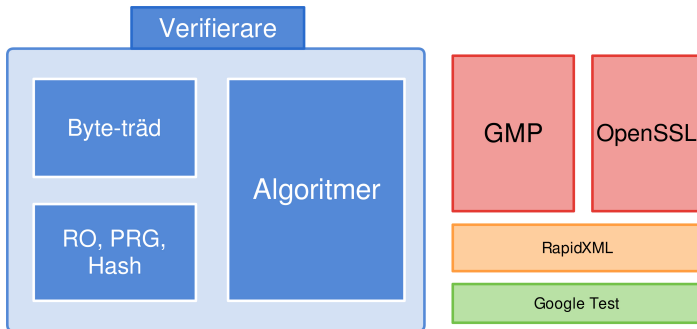
- Implementation av mixnät
- Verifierbart
- Vem som helst ska kunna verifiera
- Specifikationsdokument
  - Är det korrekt?
  - Är det användbart?

# Innehåll

- 1 Inledning
- 2 Introduktion till mixnät
- 3 Kryptografi
- 4 Mixnät
- 5 Verificatum
- 6 Implementation**
- 7 Resultat
- 8 Avslut

## Hur ser vår implementation ut?

- C++
- GMP, OpenSSL
- Representera matematiska objekt
- Verifieringsalgoritmer



# Innehåll

- 1 Inledning
- 2 Introduktion till mixnät
- 3 Kryptografi
- 4 Mixnät
- 5 Verificatum
- 6 Implementation
- 7 Resultat**
- 8 Avslut

# Hur gick det för oss?

- Bättre struktur
  - Bättre förståelse innan
  - Mer abstraktion
- Förbättring av dokumentationen
  - Tekniska fel
  - Strukturella
- Genomförbart
  - Svårt utan test

# Innehåll

- 1 Inledning
- 2 Introduktion till mixnät
- 3 Kryptografi
- 4 Mixnät
- 5 Verificatum
- 6 Implementation
- 7 Resultat
- 8 Avslut**

# Vad innebär allt detta?

- Elektronisk röstning möjligt
- Inte riktigt där *än*
- Verificatum i norska valet



# Frågor?

- Tack för att ni lyssnade!
- Har ni frågor?