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

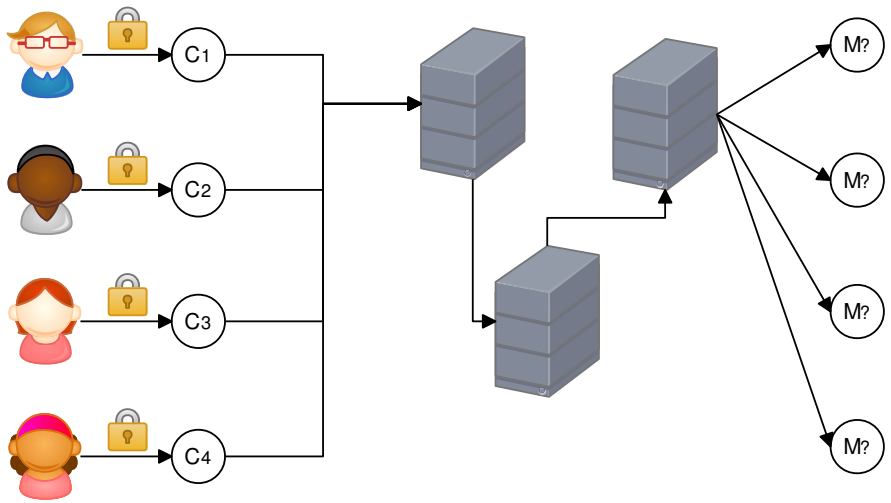
6 Implementation

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

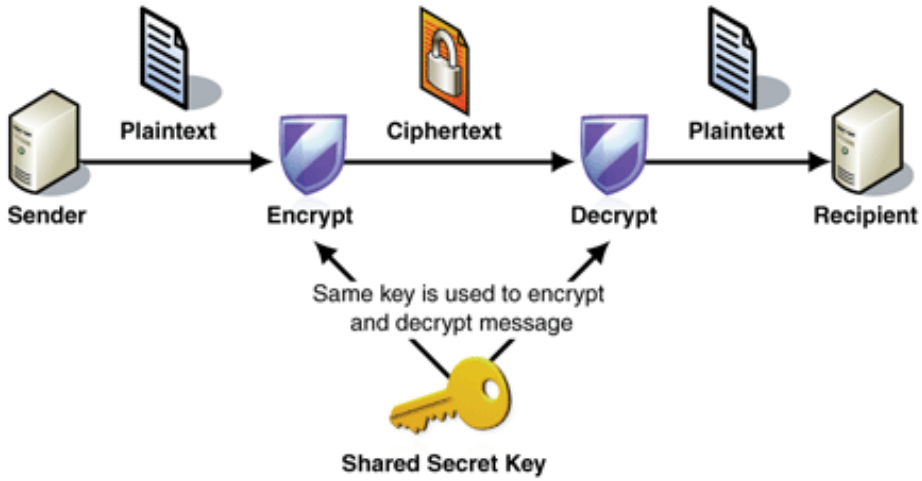
6 Implementation

7 Resultat

8 Avslut

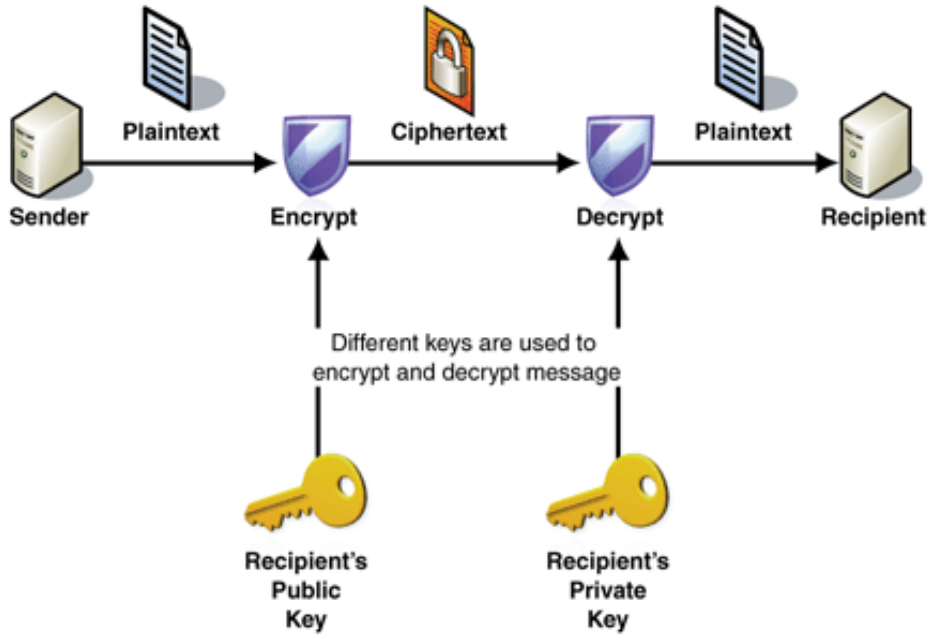
Kryptografi

- 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

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

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

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

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

Egenskaper hos El Gamal

- Lätt logaritm $\Rightarrow$ knäckt krypto.
- Homomorft
  - Möjliggör flera lager kryptering
- Generalisering till andra grupper

Zero-knowledge proof

Bevisa att man besitter information utan att avslöja informationen.
Exempel med sten, sax, påse genom kryptering.

Innehåll

1 Inledning

2 Introduktion till mixnät

3 Kryptografi

4 Mixnät

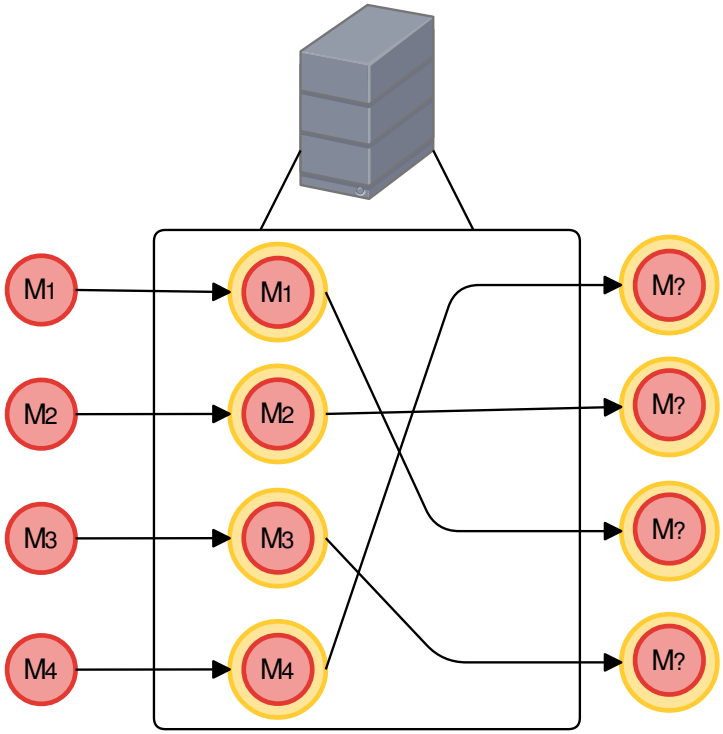
5 Verificatum

6 Implementation

7 Resultat

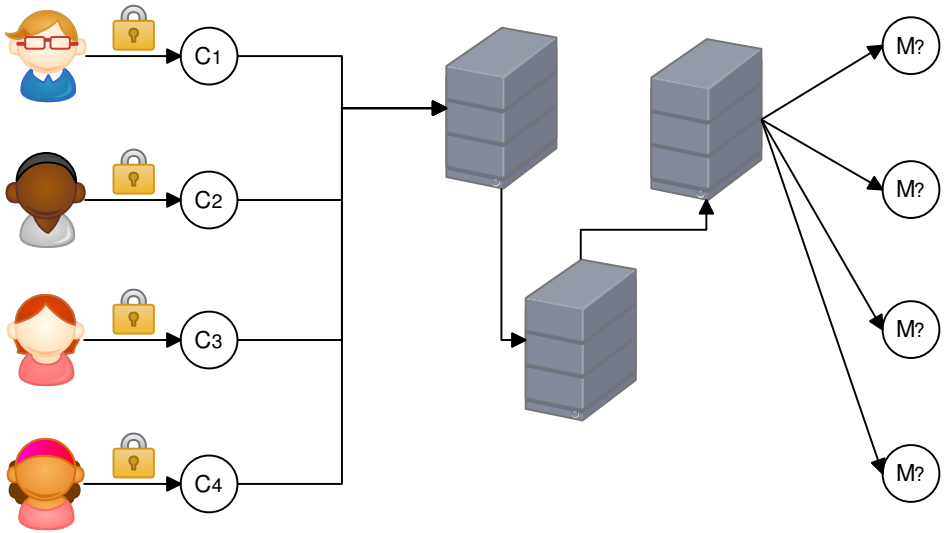
8 Avslut

Krypteringsnät



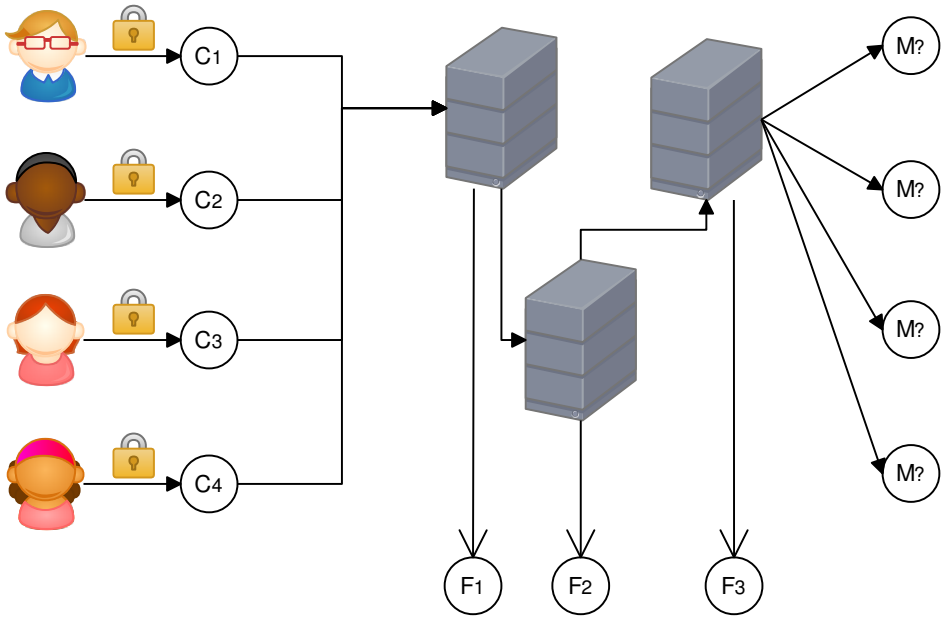
- El gamal

Verifierbarhet



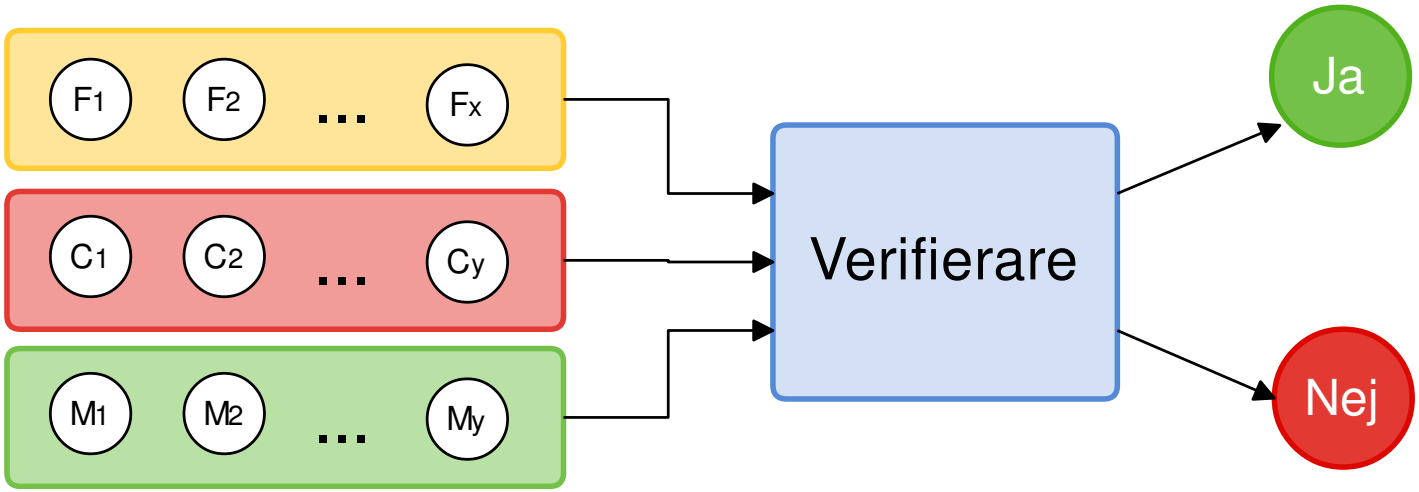
- Verifiering
- Zero-knowledge

Verifierbarhet



- Verifiering
- Zero-knowledge

Verifiering



Innehåll

1 Inledning

2 Introduktion till mixnät

3 Kryptografi

4 Mixnät

5 Verificatum

6 Implementation

7 Resultat

8 Avslut

Verifactum

Implementation, Wikström, titel, CSC

Innehåll

1 Inledning

2 Introduktion till mixnät

3 Kryptografi

4 Mixnät

5 Verificatum

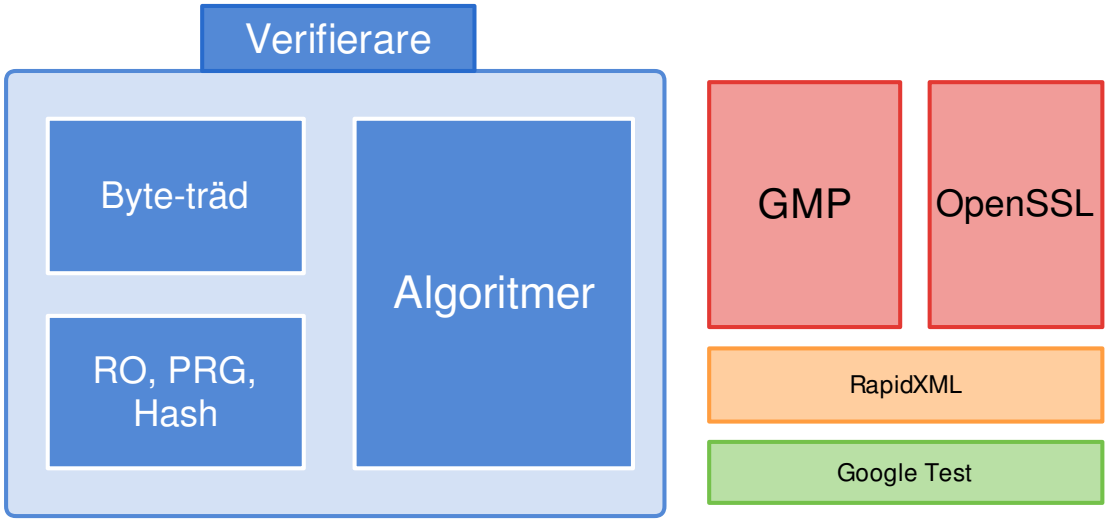
6 Implementation

7 Resultat

8 Avslut

Implementation

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



Innehåll

1 Inledning

2 Introduktion till mixnät

3 Kryptografi

4 Mixnät

5 Verificatum

6 Implementation

7 Resultat

8 Avslut

Resultat - Hur gick det?

Programmets struktur kunde varit bättre. Vi hittade fel i specifikationen. Det var genomförbart men vi kom fram med några förslag till förbättringar på dokumentet.

Innehåll

1 Inledning

2 Introduktion till mixnät

3 Kryptografi

4 Mixnät

5 Verificatum

6 Implementation

7 Resultat

8 Avslut

Roligt på slutet

Det är möjligt att skapa ett elektroniskt röstningssystem. Vi är inte riktigt där än. Verificatum kommer (antagligen) användas i nästa norska val.

Frågor?

Tack! Frågor?