El Gamal mixnät och implementering av en verifierare

Kandidatexamensarbete - SA104X - VT2013

Erik Larsson Carl Svensson
Handledare: Douglas Wikström

KTH, Skolan för datavetenskap och kommunikation

Häftigt med riksdagsval

- Rösta säkert & hemligt
- Verifierbart
- Robust

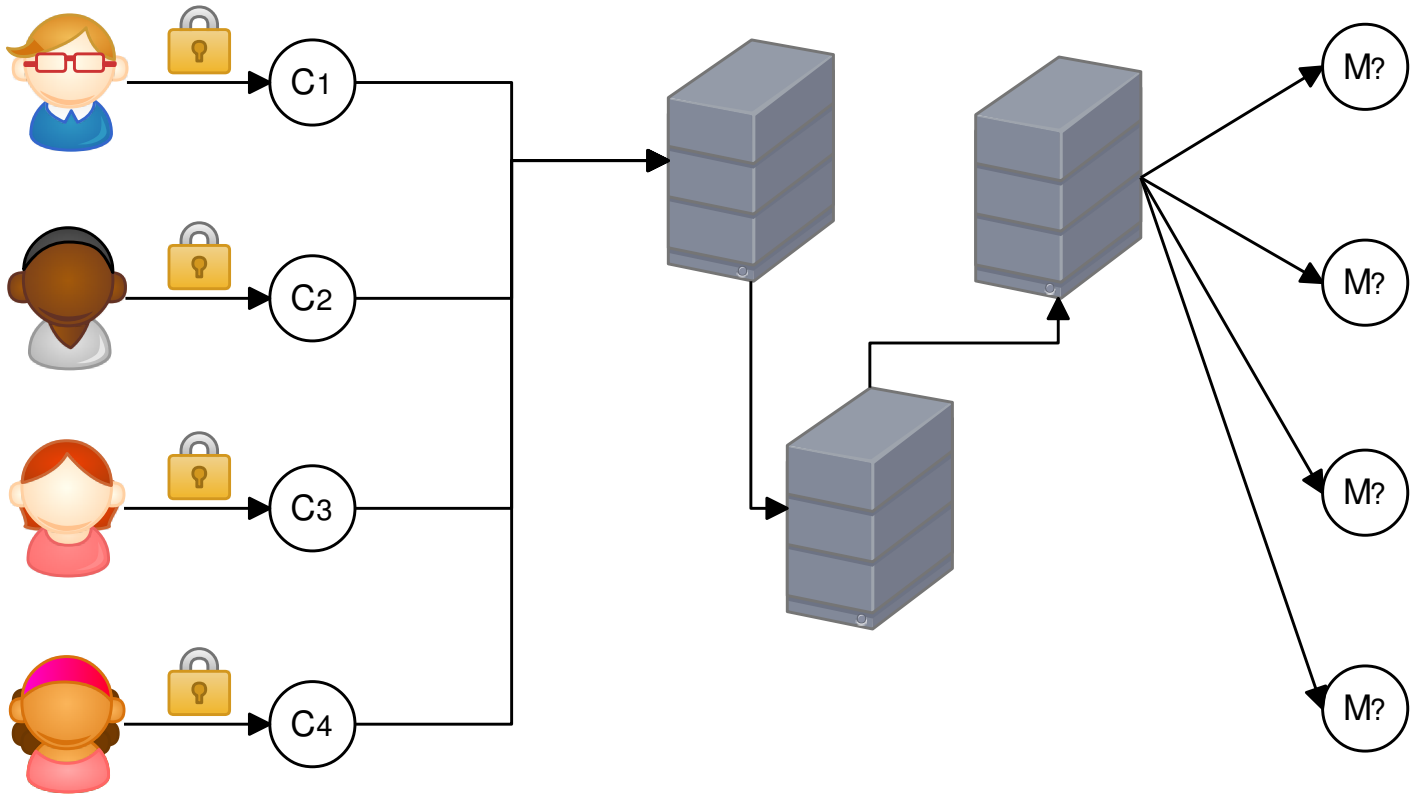
Häftigt med riksdagsval

- Rösta säkert & hemligt
- Verifierbart
- Robust
- Kanske ingen valvaka

Innehåll

Mixnät - översiktligt

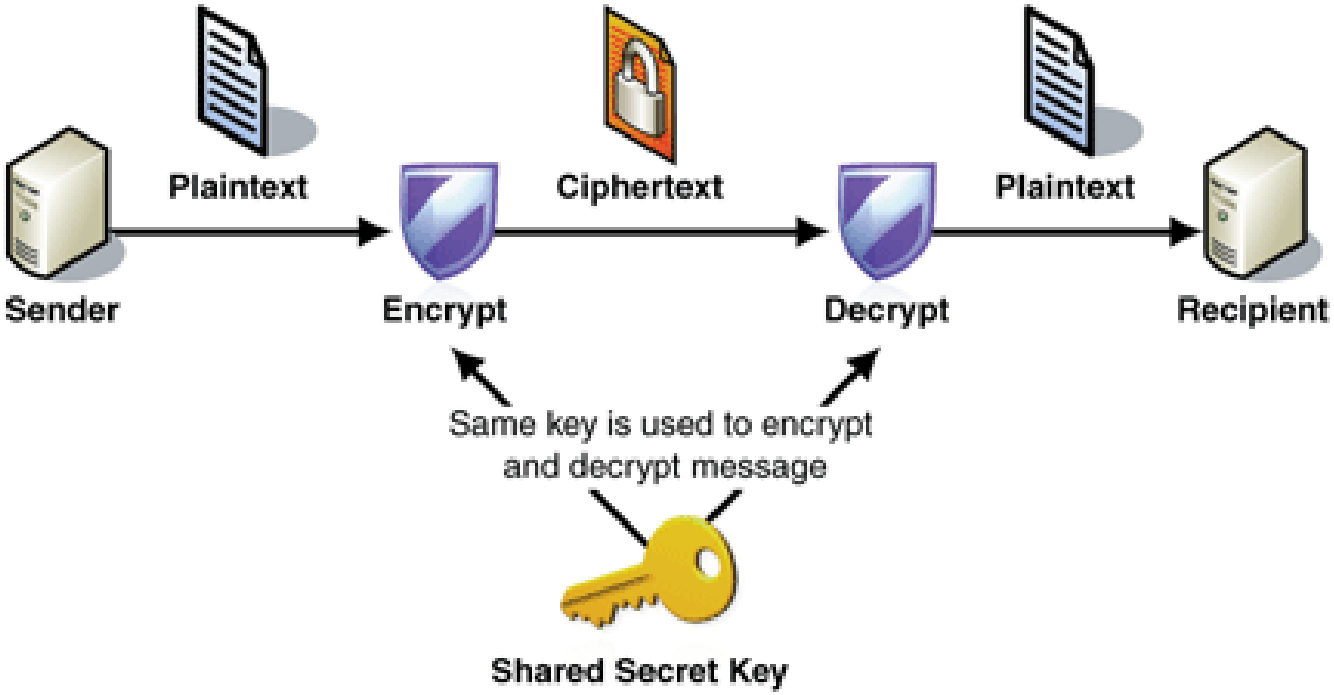
- Digital tombola



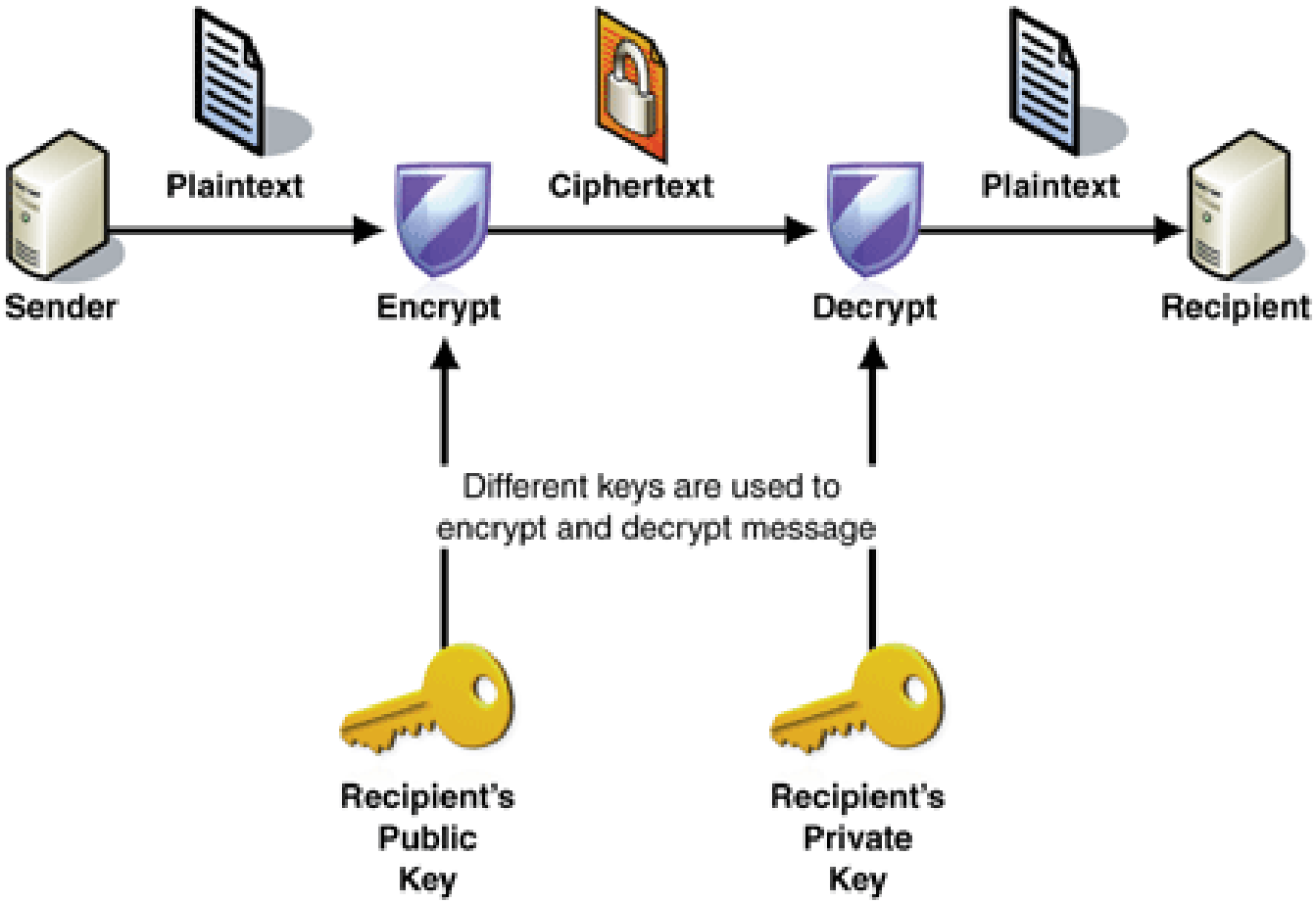
Innehåll

Kryptografi

- Första 2000 år bc.
- Public key crypto 1976



Public Key Cryptography



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

Givet y, g och p. Vad är x? Svårt! Tack vare detta så kan vi skapa El Gamal.

$$y := g^x$$

$$srandom$$

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

$$m = u^{-x} \cdot v = g^{-s \cdot x} \cdot y^s \cdot m = (g^x)^{-s} \cdot (g^x)^s \cdot m = m$$

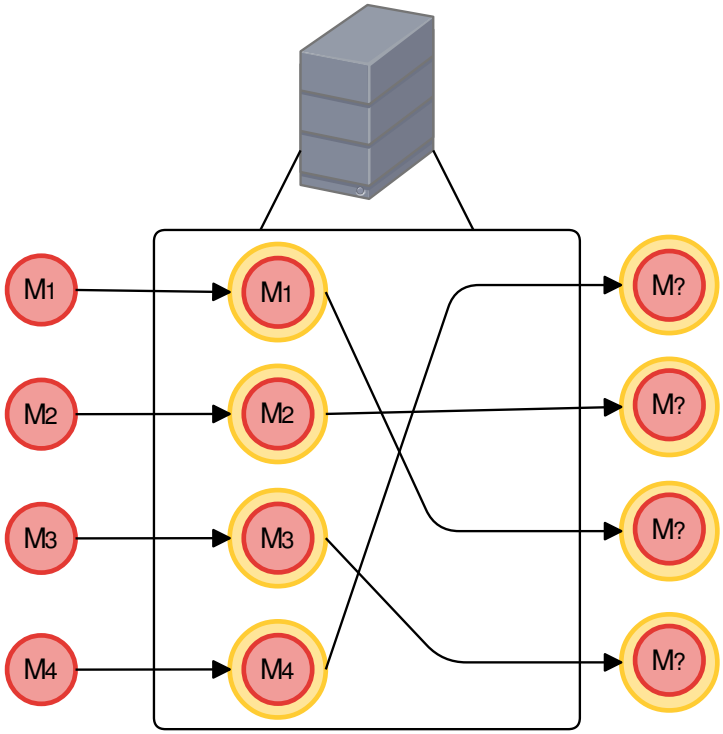
Förklara hur lätt logaritm =¿ knäckt krypto. Homomorfism, lager på lager Detta kan generaliseras till valfri cyklisk grupp.

Zero-knowledge proof

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

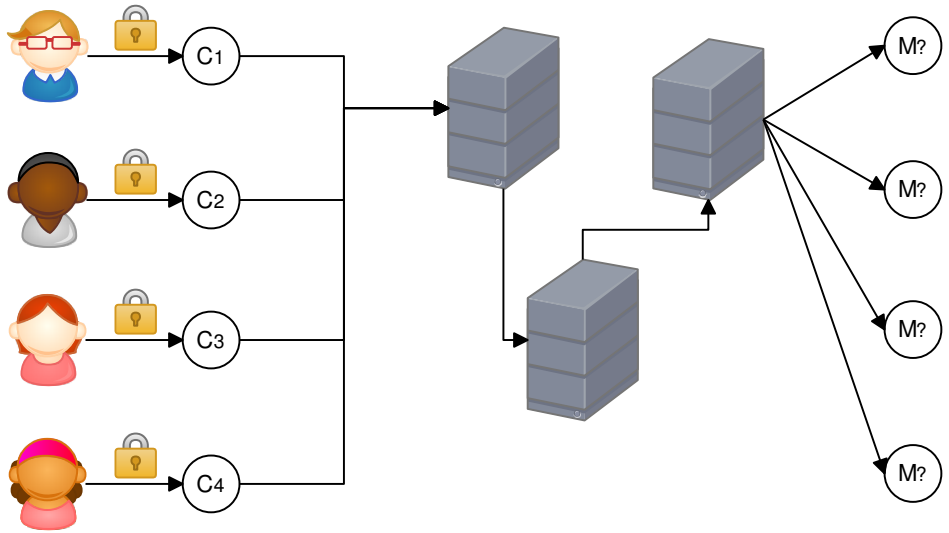
Innehåll

Krypteringsnät



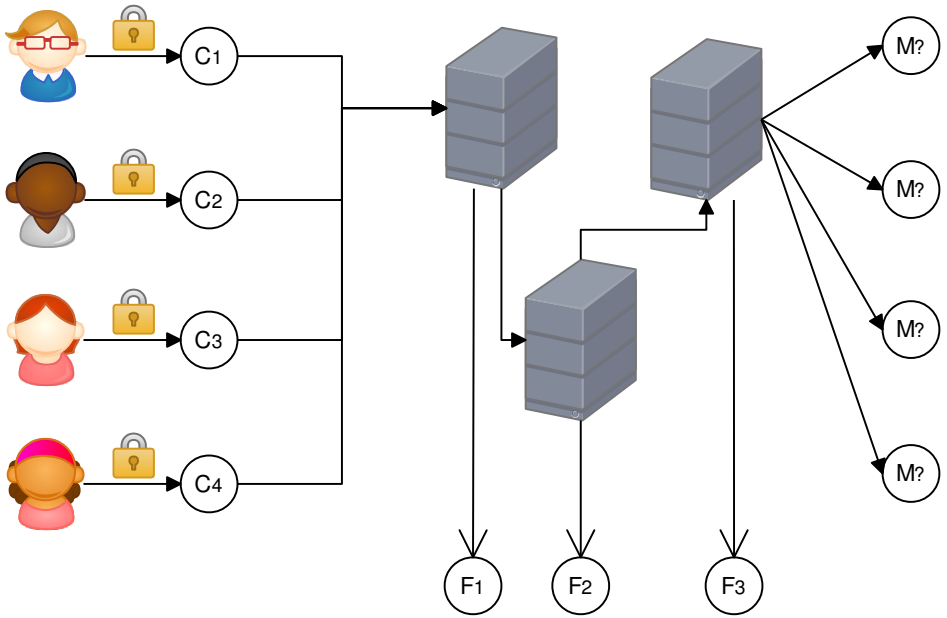
- El gamal

Verifierbarhet



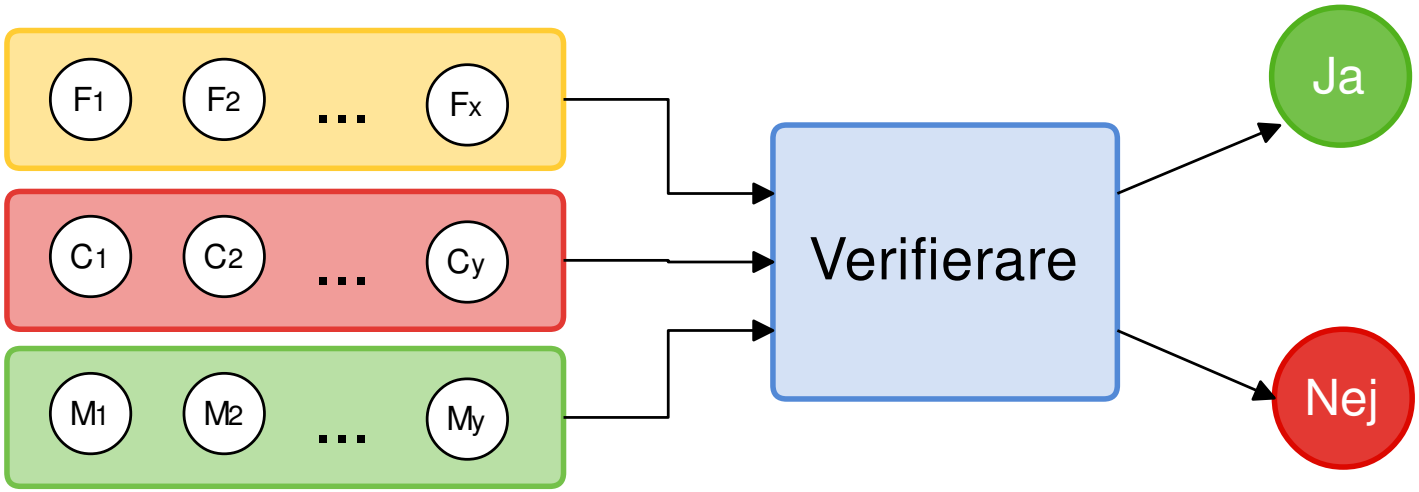
- Verifiering
- Zero-knowledge

Verifierbarhet



- Verifiering
- Zero-knowledge

Verifiering



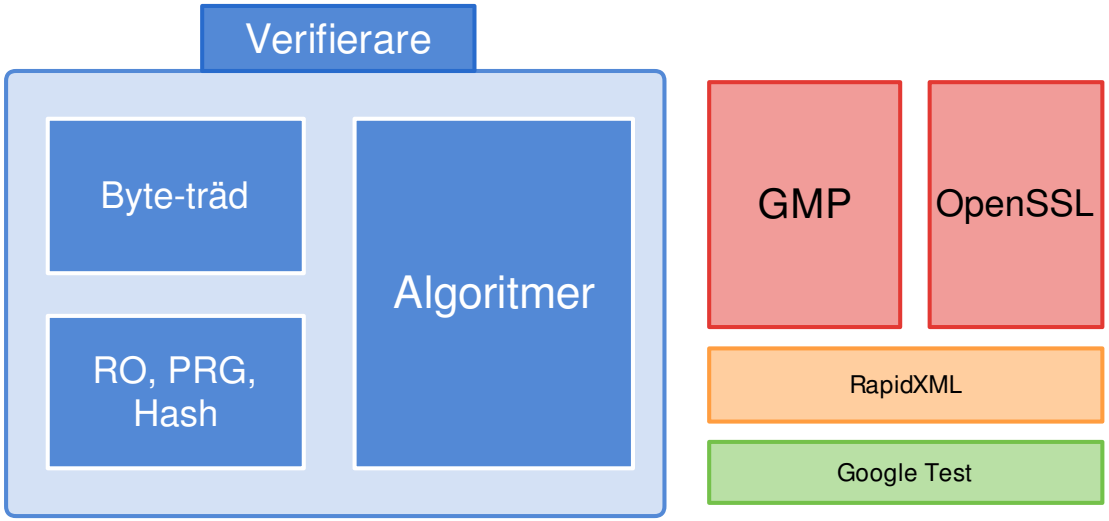
Verifactum

Implementation, Wikström, titel, CSC

Innehåll

Implementation

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



Innehåll

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

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?