Hur jag slutade ängslas och lärde mig älska krypto

OWASP JKPG

2020-10-08

19:00

Broadcast on YouTube: https://youtu.be/HEB41hchym0

Jonathan Jogenfors

- Infosäk-konsult på Atea i Jönköping
- Tidigare: Sectra Communications
- PhD + postdoc i kvantkrypto, LiU
- Med och driver OWASP JKPG

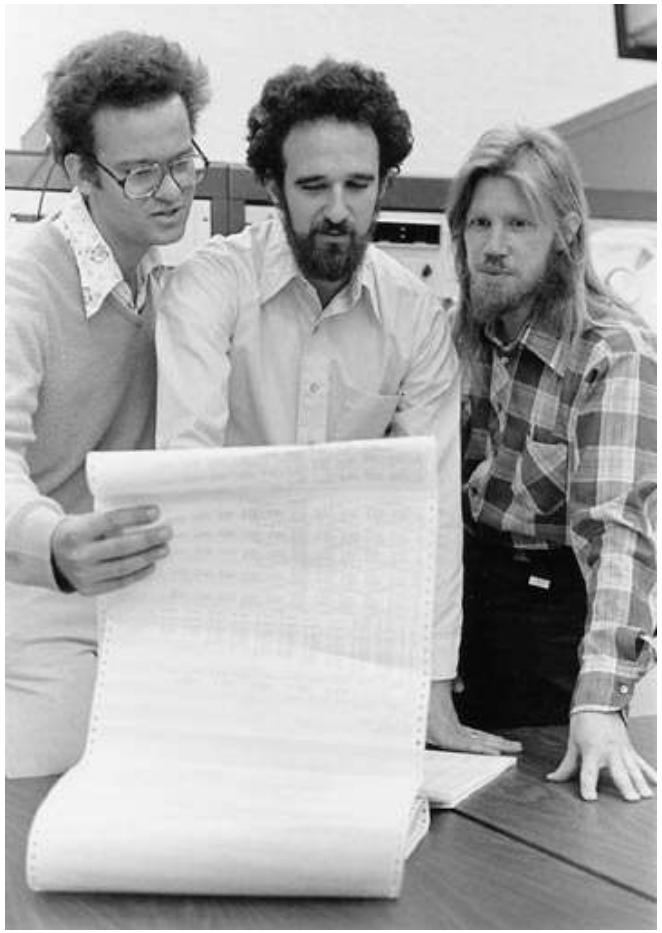
- Twitter: @Jogenfors

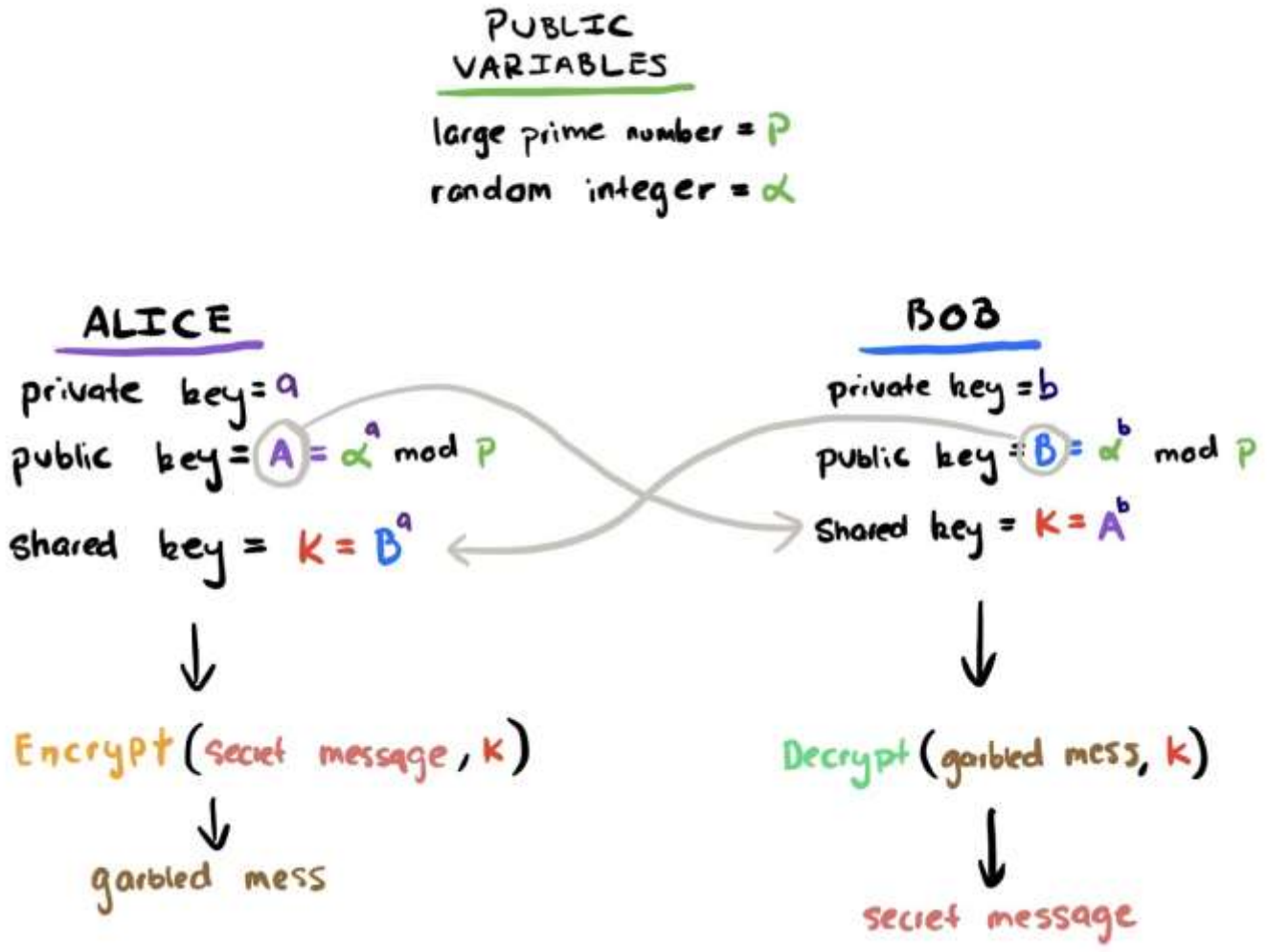
Symmetriskt krypto

Kerckhoff’s princip

- “Endast nyckeln ska vara hemlig”
- Det finns undantag till denna regel

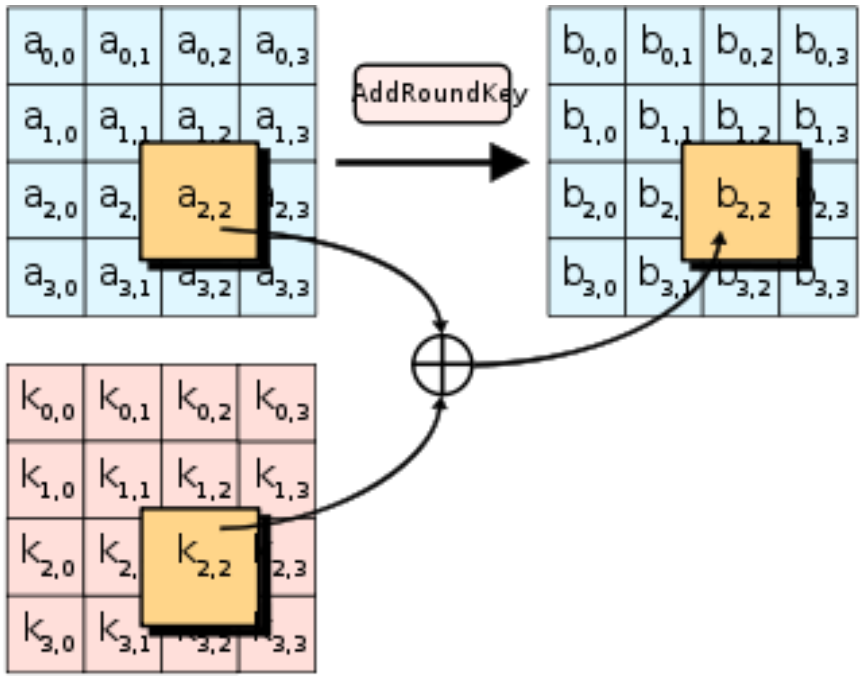
Diffie-Hellman (1976)



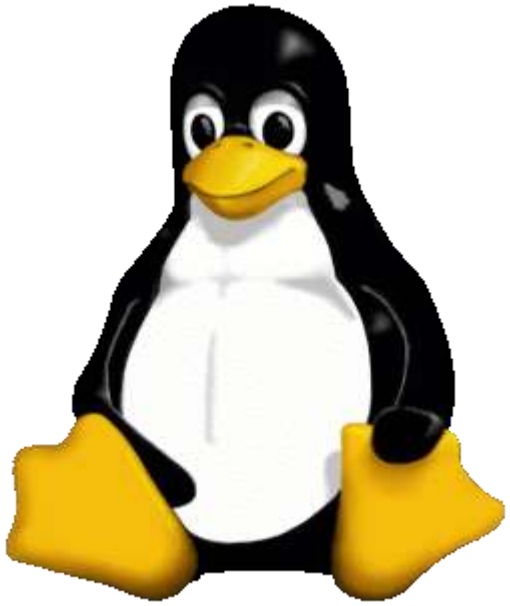


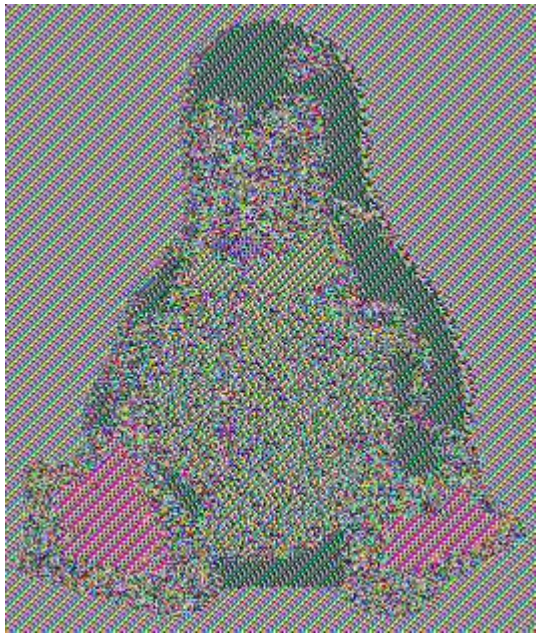
AES: den moderna arbetshästen

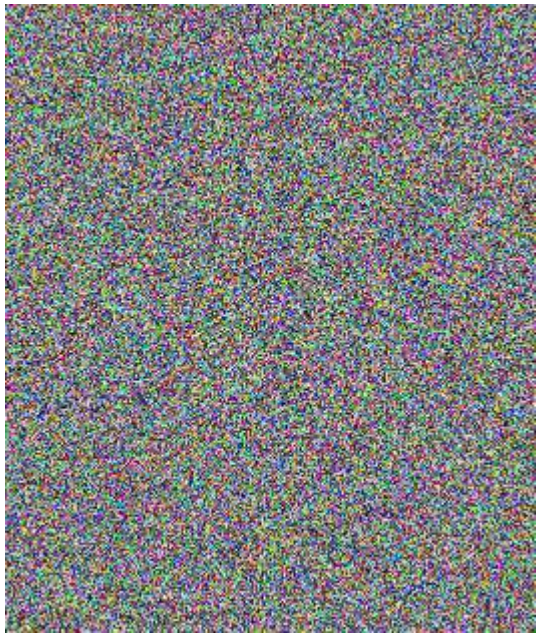
- Advanced Encryption Standard standardiserades av NIST 2001
- Snabbt i hårdvara och mjukvara
- Säker!
- Blockkrypto



Hur använder man ett blockkrypto?







Nyckelhantering

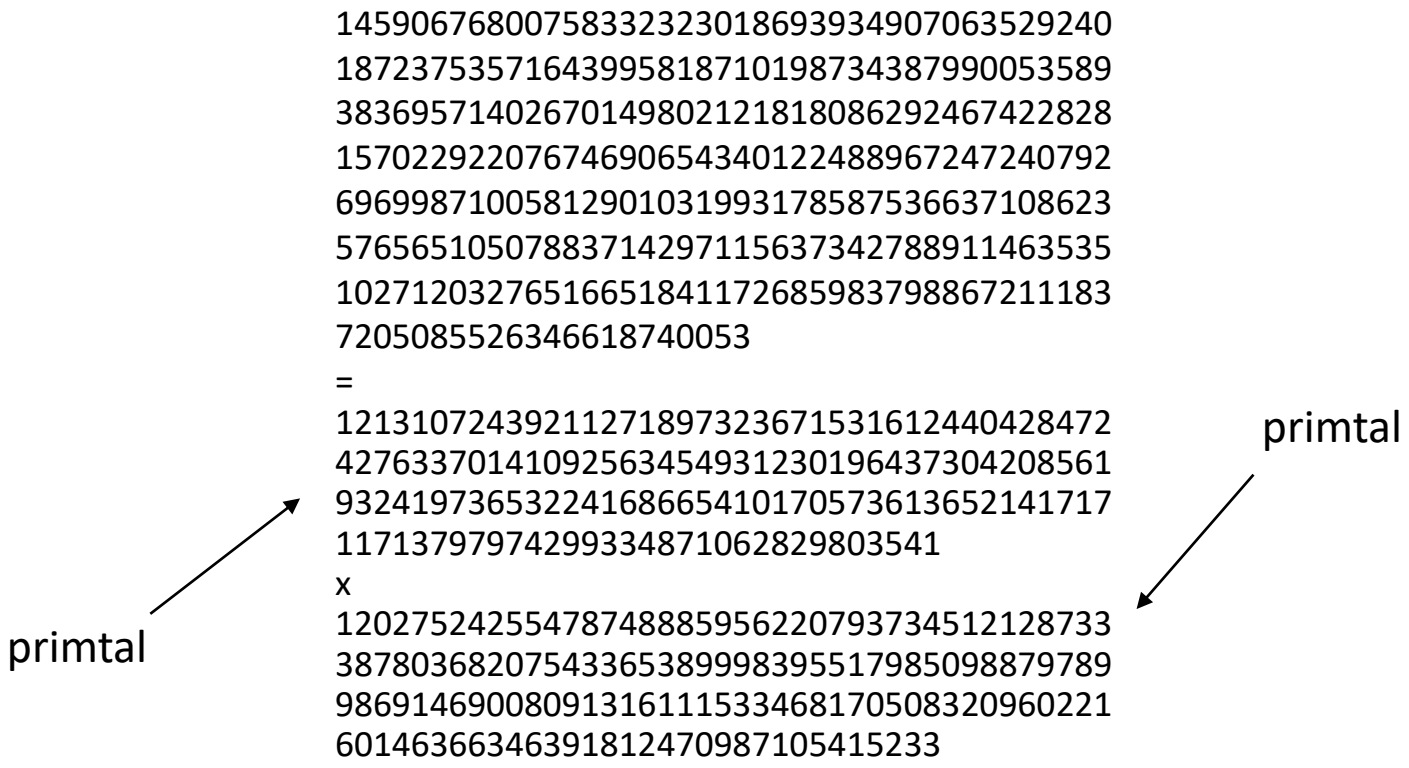
- Dyrt och svårt!

Trapdoor-funktioner

- Enkelt att gå åt ena hållet
- Svårt åt andra hållet

- Enkelt att gå åt båda hållen med en hemlig bit information

Primtalsfaktorisering, n=pq



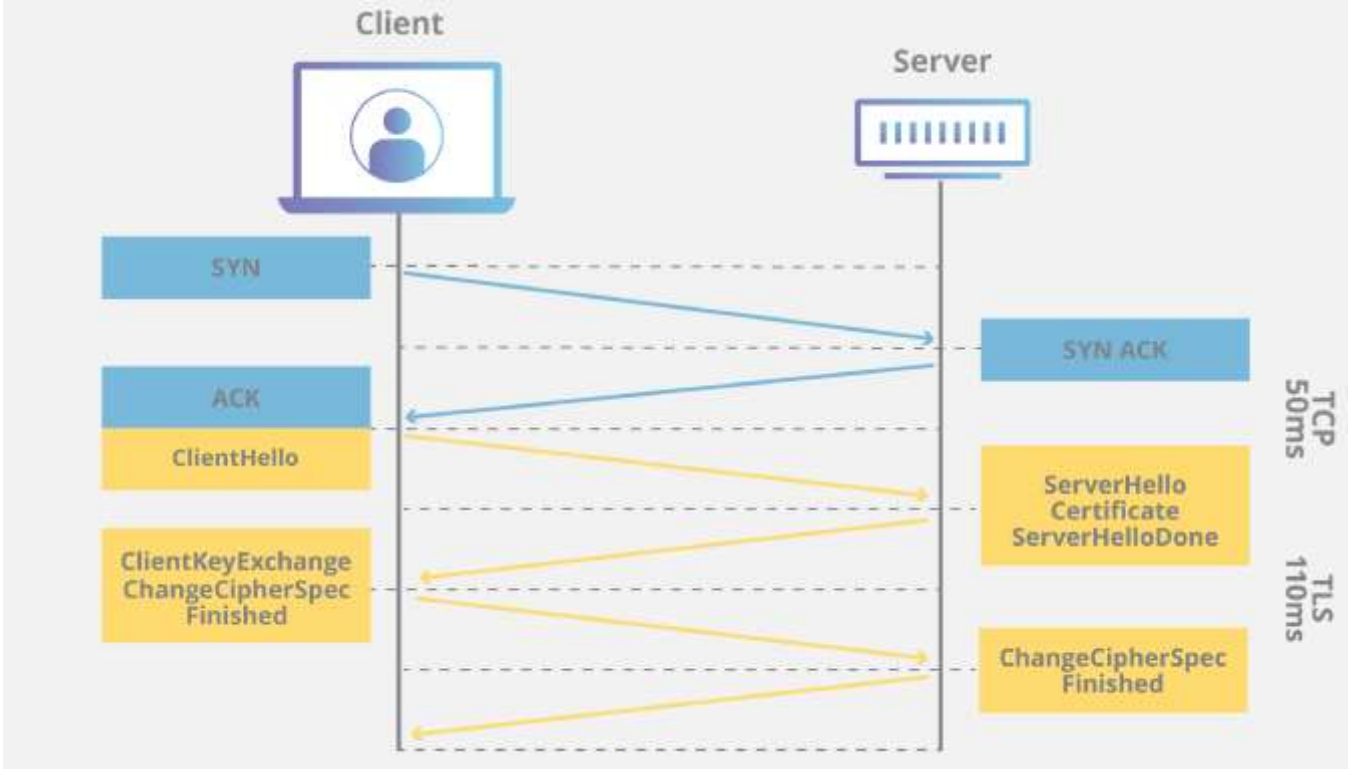
- Lätt att multiplicera
- Svårt att faktorisera

Symmetriskt vs asymmetriskt

- Symmetriskt krypto: Snabbt, säkert och enkelt att studera, kräver nyckel
- Asymmetriskt krypto: Långsamt, svår matematik
- Sessionsnyckel

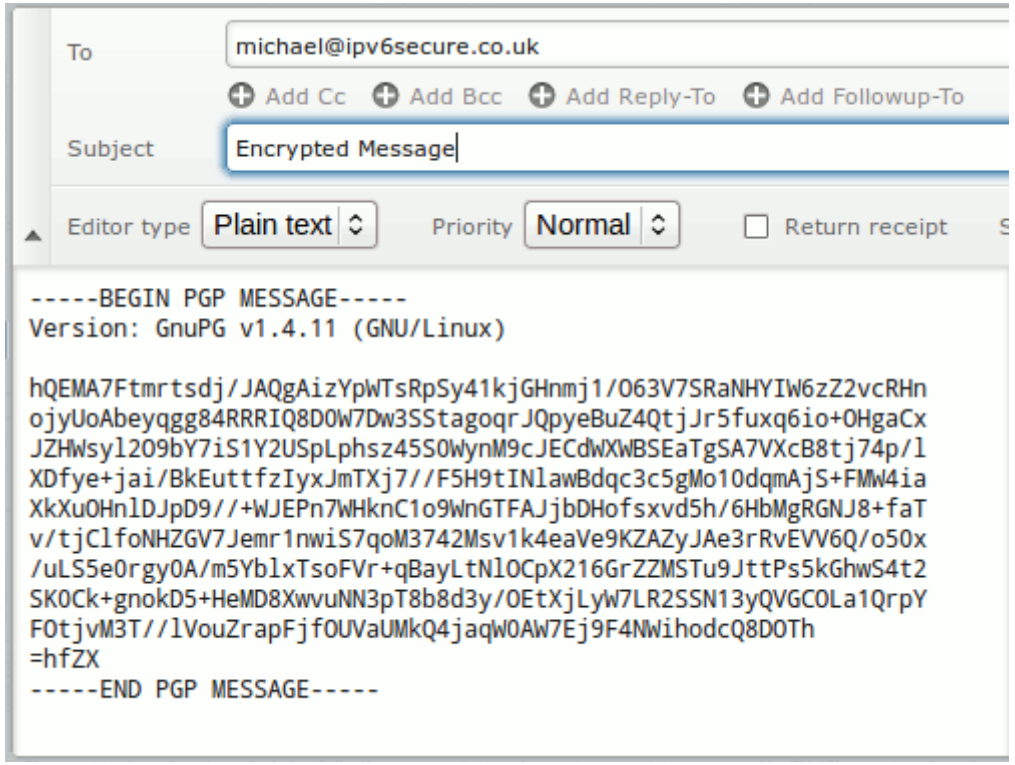
Exempel: TLS/HTTPS

- Förmodligen det viktigaste kryptoprotokollet idag
- Senaste versionen är TLS1.3, TLS1.2 är OK
- TLS1.0 och TLS1.1 är förlegade



Gamla tiders krypto: PGP/GPG

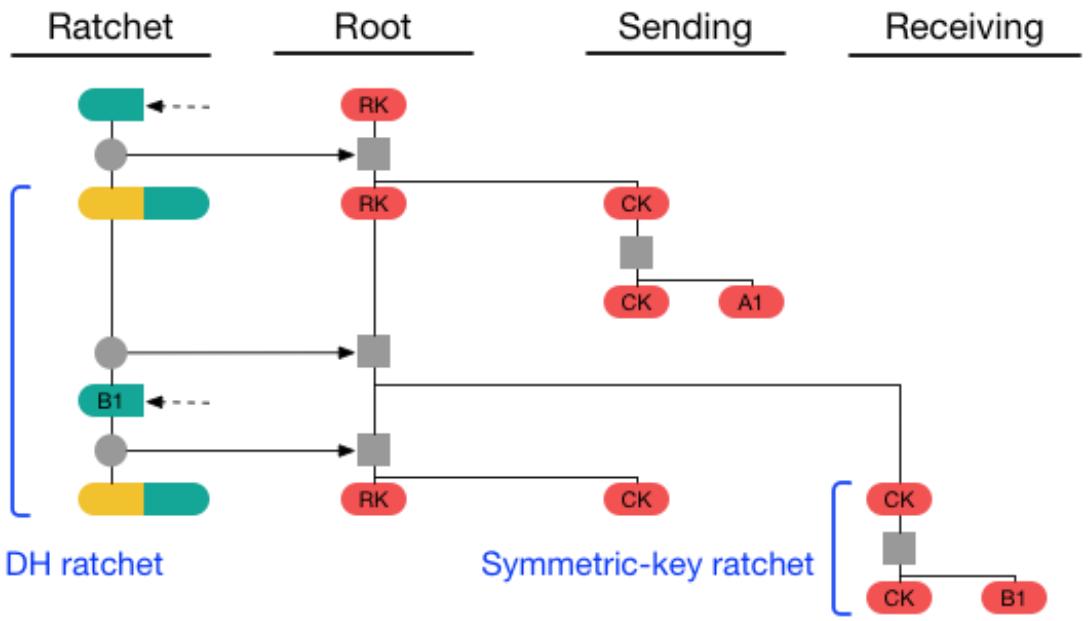
- GPG ger e-postsäkerhet
- Varje person har ett nyckelpar
- Web of trust
- “a glorious experiment that has run its course”



Ny tiders krypto: Forward Secrecy

- “Nya nycklar varje gång”
- Förlorar man en nyckel kan man inte dekryptera tidigare meddelanden

- Bra exempel: Signal



Informationssäkerhet behöver krypto

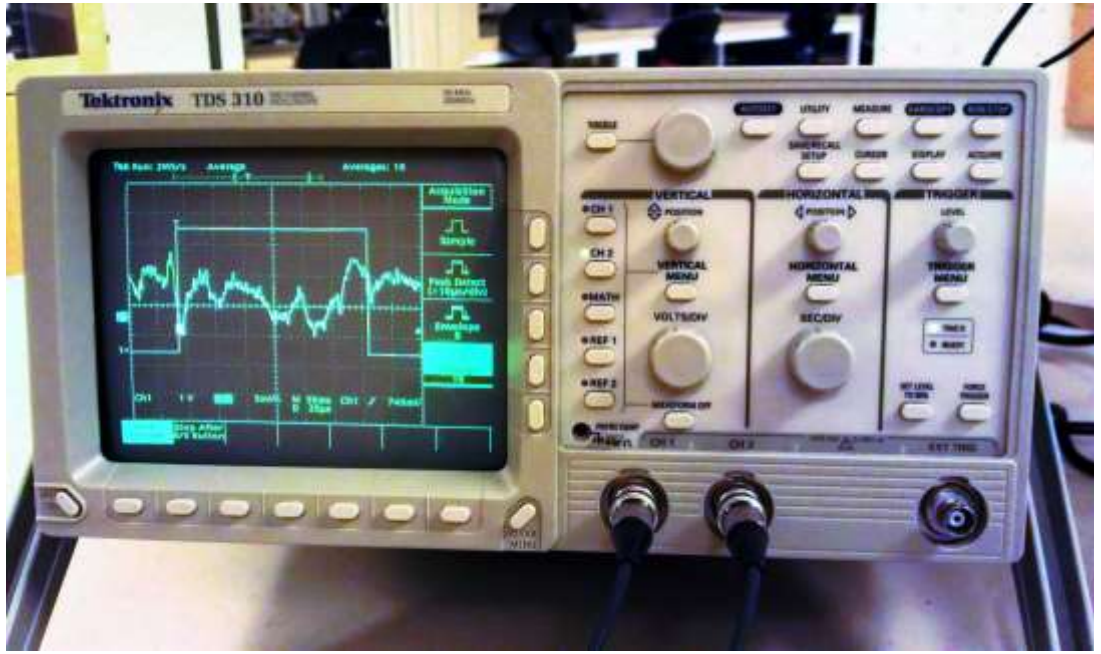
- Sekretess (uppenbart)
- Riktighet (checksummor)
- Tillgänglighet (mer komplext)
- Non-repudiation (signaturer)

Hur knäcker man krypto?

- De senaste 50 åren har algoritmerna blivit “för bra” för att knäckas
- I stället ger man sig på ändpunkterna

Knäcka krypto: Power Analysis

- Mät strömförbrukningen hos kryptochipet
- Väldigt relevant för smartkort



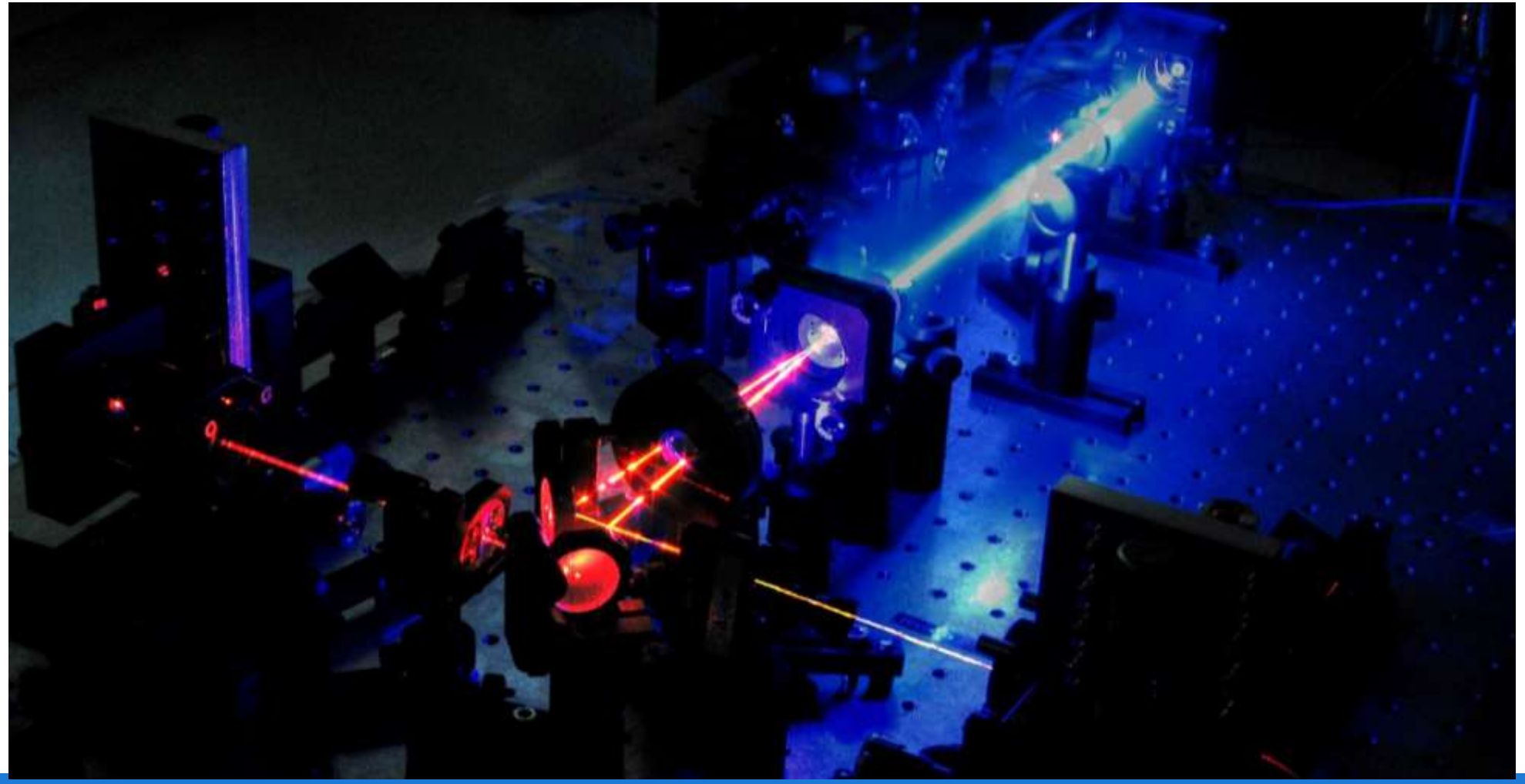
Exempel: Krypterad rösttrafik

Autentisera ditt krypto!

- Kryptering ger inte Riktighet
- Autentisering ger inte Sekretess
- AEAD, Authenticated Encryption with Associated Data

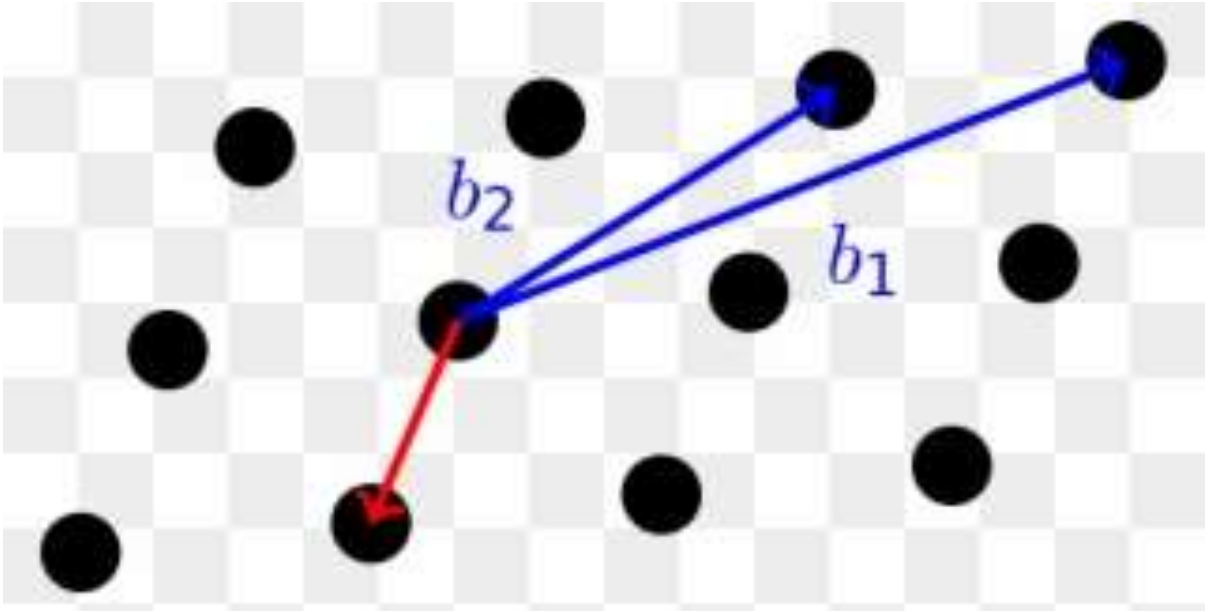
Hot mot krypto: Kvantdatorer

Kvantkrypto, en möjlig lösning?



Kvantsäkert krypto

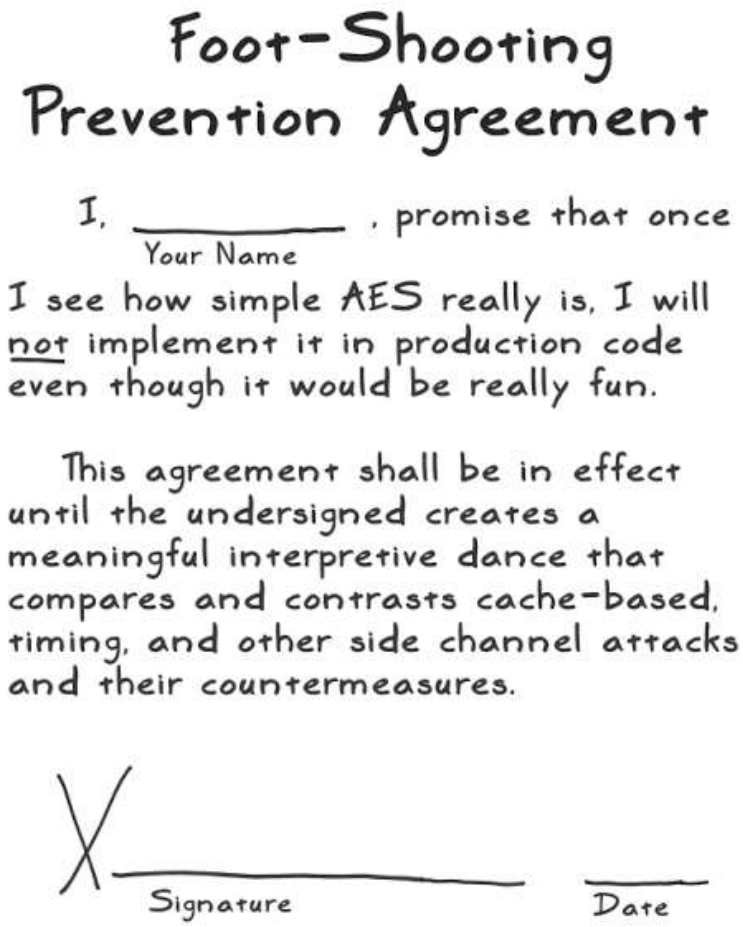
- Kvantdatorer förstör våra existerande trapdoor-funktioner
- Behövs ny matematik
- Lattice-krypto
- Kod-krypto



Defense in depth

- Säkerhet är som en lök, ju mer du tar bort desto mer gråter du

Implementera inte krypto själv



Foot-Shooting
Prevention Agreement

I, _____ , promise that once
Your Name
I see how simple AES really is, I will
not implement it in production code
even though it would be really fun.

This agreement shall be in effect
until the undersigned creates a
meaningful interpretive dance that
compares and contrasts cache-based,
timing, and other side channel attacks
and their countermeasures.

X _____ _____
Signature Date

Iota: Bra exempel på hur det inte ska göras

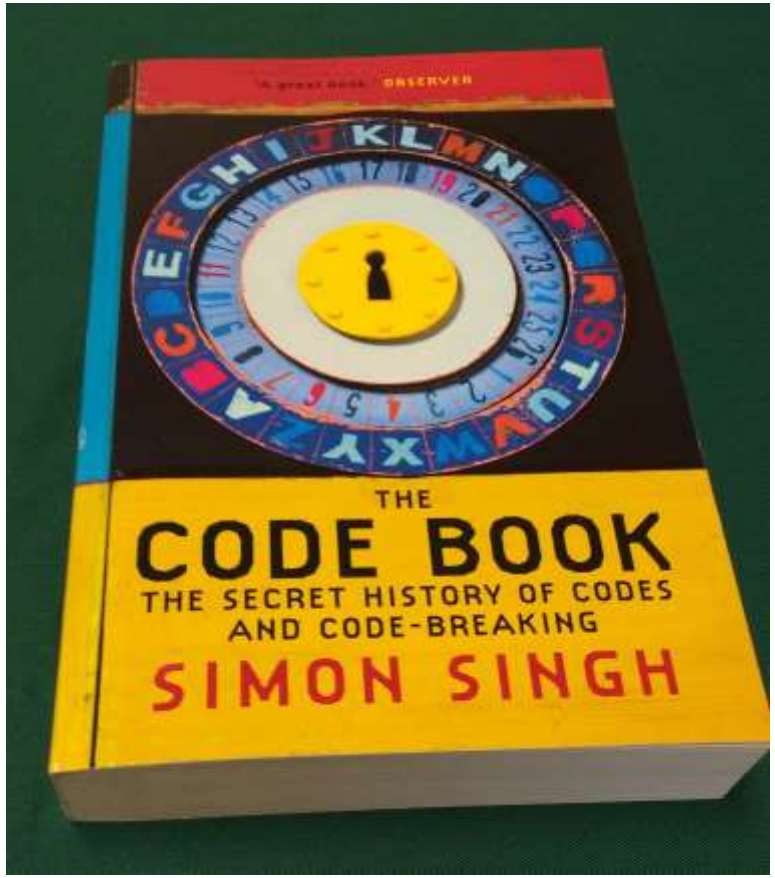
```
117
118       var normalizedHash = this.normalizedBundle(hash);
119       if(normalizedHash.indexOf(13 /* = M */) != -1) {
120         // Insecure bundle. Increment Tag and recompute bundle hash.
121         var increasedTag = tritAdd(Converter.trits(this.bundle[0].obsoleteTag), [1]);
122         this.bundle[0].obsoleteTag = Converter.trytes(increasedTag);
123       } else {
124         validBundle = true;
125       }
```

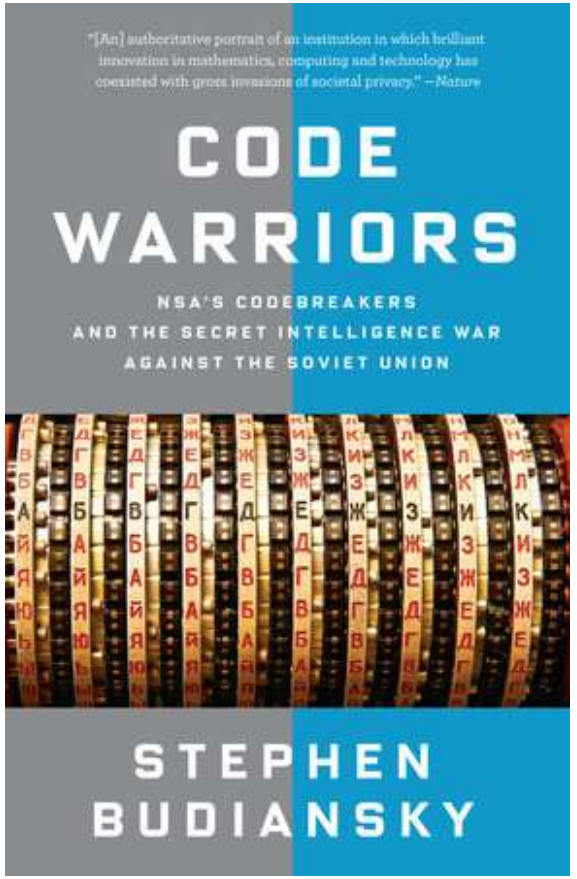
- https://github.com/iotaledger/iota.js/blob/0927cdd94f496ca1939d0b885a6b513a0b8c5aa5/lib/crypto/bundle/bundle.js#L119

Libsodium

- Bra sätt att använda krypto
- Går inte att göra fel

Boktips!


THE
CODE BOOK
THE SECRET HISTORY OF CODES
AND CODE-BREAKING
SIMON SINGH


"[An] authoritative portrait of an institution in which brilliant
innovation in mathematics, computing and technology has
coexisted with gross invasions of societal privacy." —Nature
CODE
WARRIORS
NSA'S CODEBREAKERS
AND THE SECRET INTELLIGENCE WAR
AGAINST THE SOVIET UNION
STEPHEN
BUDIANSKY

Social engineering - You are a target

19 november 2020, 19:00

Virtuellt event