

2015-11-05, VabaLava

Krüptograafia eluiga

Anto Veldre, RIA.ee



Millest täna räägime

- Ajalugu, lahtiütlemised, kaastundeavaldused
- Kuulujutud ja teadustööd
- Kohutava turva-aasta 2014 järelmid
- Tehnoloogia arengust, muutumis(t)e kiirusest
- Vajadus uuendada?
- Veeuputusjärgne/*postquantum* krüpto*
- Tungiv vajadus pidevalt uuendada!!



Disclaimer



of all pictures belong
to their respective owners



Disclaimer (2)

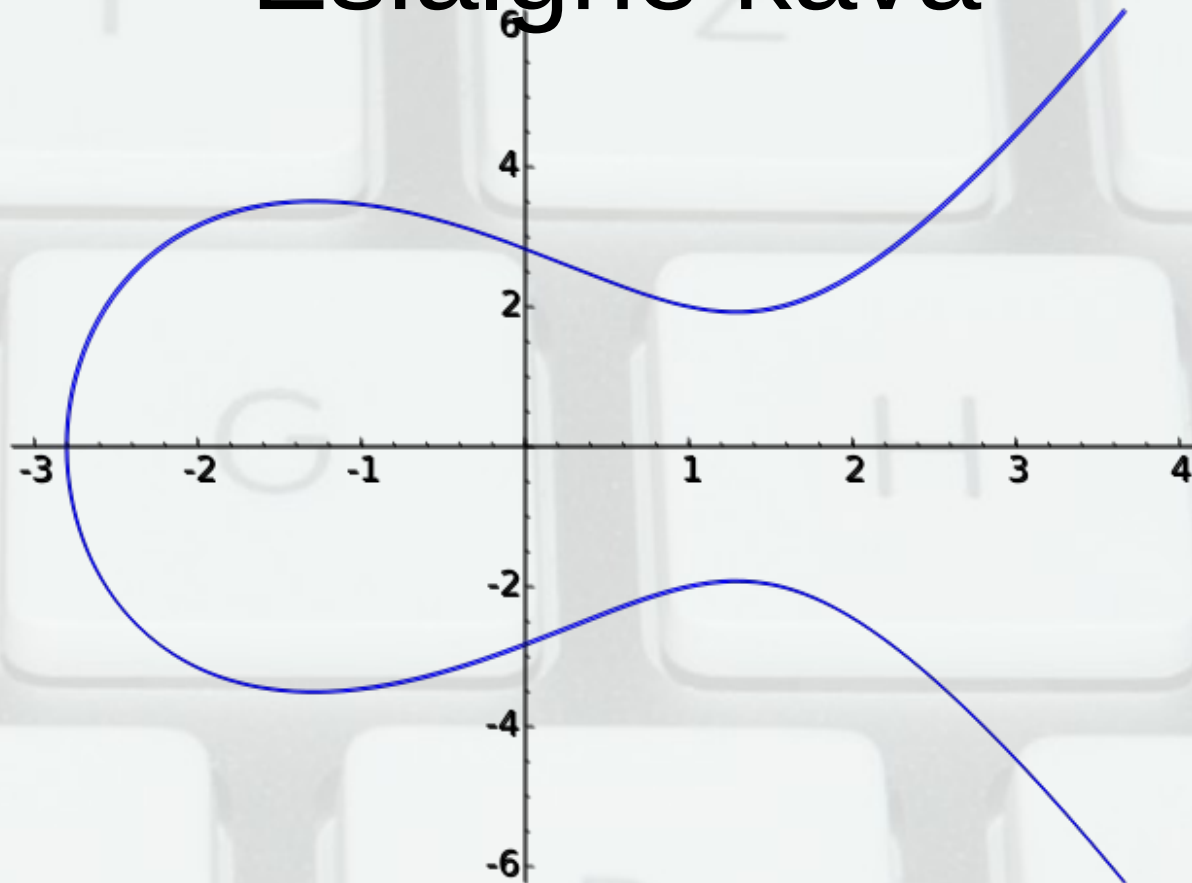


Riigi Infosüsteemi Ameti analüütik hoiatab:

- Ärge üritage kodus luua omaenda krüptograafiat ega omapäi parandada olemasolevat! Vajadusel pöörduge abi ja nõuannete saamiseks elukutselise krüptograafi poole.
- Kahjulike sümptomite jätkumisel või ravi kõrvalnähtude ilmnemisel soovitame võtta ühendust CERT-EE ja Politseiga.

NB! Anto ei ole krüptograaf

Esialgne kava



Joonis 1. Elliptikõver $y^2 = x^3 - 5x + 8$ üle reaalarvude

2011
2013
2015

In Estonia in total:



1,151 incidents handled
(1164 in 2013)



22 denial-of-service attacks
(13 in 2013)



295 defacement incidents
(240 in 2013)



127 quarterly summaries and incident reports
submitted to RIA (73 in 2013)

In state institutions:



486 incidents in state institutions
(135 in 2013)

The most common reasons for incidents:

- attacks
- power cuts
- data communication disruptions
- software malfunctions



20% of reported incidents were highly critical.



Dangerous vulnerabilities:

Heartbleed and Shellshock



23 cyber security training events,

total number of participants 744



International cyber exercises:

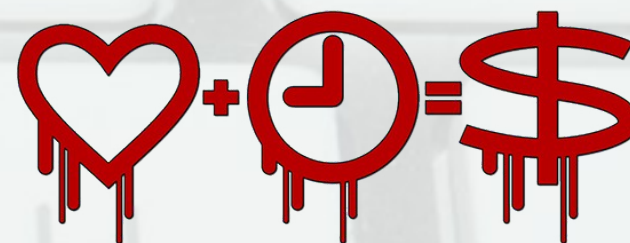
Cyber Europe, Cyber Coalition and Locked Shields



60% of people in Estonia use smart devices.

75% of children say, "My parents are not interested in what I do on my smart device."

Aasta 2014 kokkuvõte



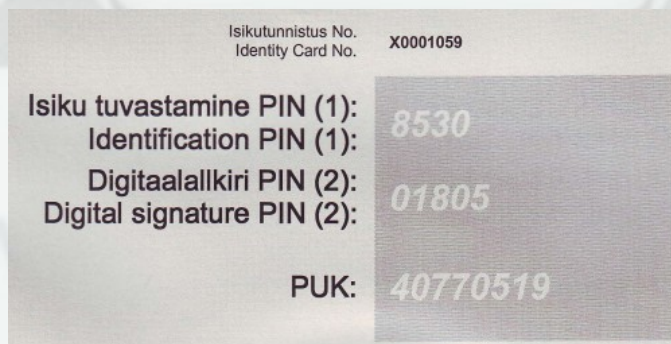
LaMontagne
Cartoonists.com

BoringSSL

Libre SSL



Maailm ja 2FA



+



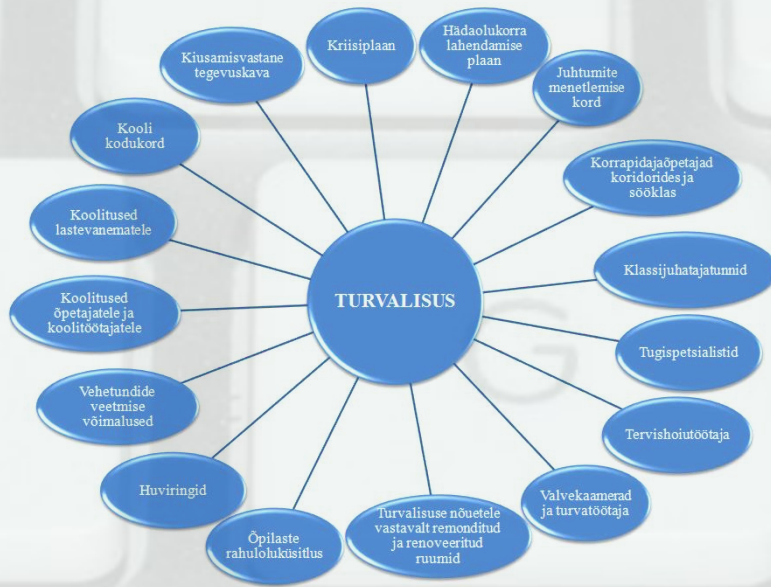
STOP
ID
THEFT



Eesti iseärasused



Turvalisus



e-ühiskond peab töötama!





UPDATE

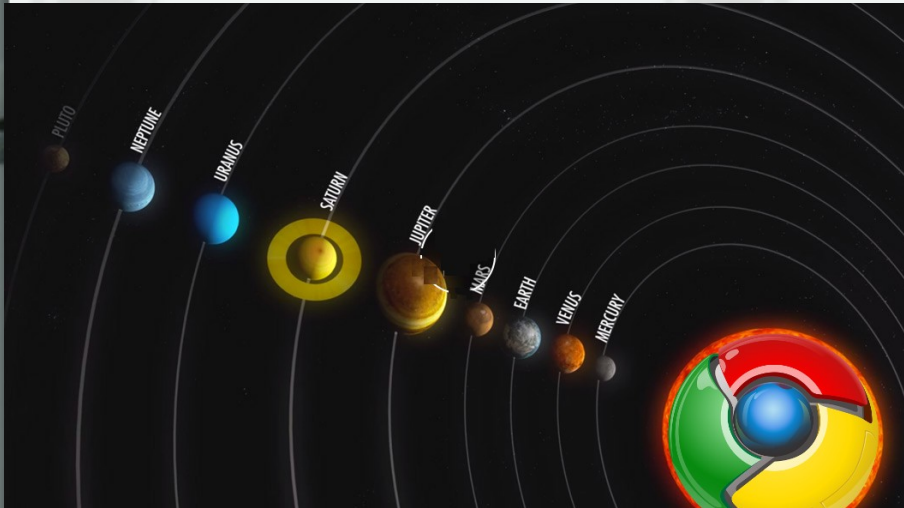
UPDATE



UPDATE



Brauserikeskne maailm



OpenSSL
Cryptography and SSL/TLS Toolkit

BoringSSL

Teal's Spaghetti Alla Carbonara

Ingredients

- thick pancetta or parma ham
- eggs yolks
- ½ cup grated parmesan cheese
- ½ cup cream
- ground pepper
- cooked pasta

Directions

- Chop it up, cook and lightly drain. Leave bacon in pan, and set aside.
- Beat yolks. Add cheese and fresh ground pepper to taste. Mix into a dough-like consistency. Add cream – mix thoroughly and set aside.
- Toss and warm cooked pasta in the bacon pan.
- Add sauce to pan and toss – simmer for only about 60-90 seconds
- Top with more parmesan and pepper and think of Italy.
- Drink wine copiously.

Brauserikeskne maailm



Randy Brito @randybrito · 13h

So am I unable to login to the e-Resident web due to this? [news.postimees.ee/3348383/all-e- ...](https://news.postimees.ee/3348383/all-e-...) or something else? @cfarivar @KeberNeet @ronaldiive



- eggs
- ½ cup grated parmesan cheese
- ½ cup cream
- ground pepper
- cooked pasta

Directions

- Chop it up, cook and lightly drain. Leave bacon in pan, and set aside.
- Beat yolks. Add cheese and fresh ground pepper to taste. Mix into a dough-like consistency. Add cream – mix thoroughly and set aside.
- Toss and warm cooked pasta in the bacon pan.
- Add sauce to pan and toss – simmer for only about 60-90 seconds
- Top with more parmesan and pepper and think of Italy.
- Drink wine copiously.

Kuidas olla turvaline
pikas perspektiivis?



UPDATE

Pole ju väga uus asi?

ID-kaardi haldusvahend

ID-kaardi
HALDUSVAHEND

Diagnostika Seaded Abi Info Estonian ▼



Nimi: Mari-Liis Männik
Isikukood: 47101010033
Sündinud: 01. jaanuar 1971, Eesti / Est
Kodakondsus: EST
E-post: mari-liis.mannik.13@eesti.ee

[Laadi pilt](#)

Sertifikaadid

@eesti.ee e-post

Mobiil-ID

PUK kood

Lugejas on dokument AS0010541
See on **kehtiv** dokument
Kaart on kehtiv kuni 21. august 2016

Isikutuvastamise sertifikaat
Sertifikaat on **kehtiv ja kasutatav**
Sertifikaat kehtib kuni 21. august 2016
Sertifikaat aegub 41 päeva pärast
Sertifikaati on kasutatud isikutuvastamiseks 4 korda

Allkirjastamise sertifikaat
Sertifikaat on **kehtiv ja kasutatav**
Sertifikaat kehtib kuni 21. august 2016
Sertifikaat aegub 41 päeva pärast
Sertifikaati on kasutatud allkirjastamiseks 2 korda

Uuenda sertifikaate

Muuda PIN1 Vaata üksikasju

Muuda PIN2 Vaata üksikasju



Mida maailmas veel toimub?

Taavi Rõivas: ID-kaardi turvalisuse nõrgestamine tagaukse kaudu ei ole Eestile vastuvõetav (4)



(Foto: Martin Dremļuga/ERR)

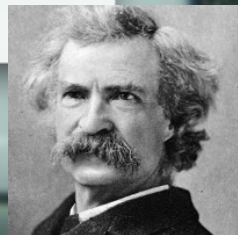


Cameron wants to ban encryption - he can say goodbye to digital Britain

James Ball



Online shopping, banking and messaging all use encryption. Cameron either knows his anti-terror talk is unworkable and is looking for headlines, or he hasn't got a clue



Aus mees, lubas kokku ja tegigi ära!



[Draft Investigatory Powers Bill](#)

Ref: ISBN 9781474125666, ID 30101501 11/15
PDF, 3.38MB, 299 pages

This file may not be suitable for users of assistive technology.
[Request a different format.](#)

The bill notes that an existing 2000-signed law, the Regulation of Investigatory Powers Act (RIPA), requires communication service providers -- which includes tech firms -- to "provide communications data when served with a notice, to assist in giving effect to interception warrants, and to maintain permanent interception capabilities, including maintaining the ability to remove any encryption applied by the [company] to whom the notice relates."



Turvaline kodu - Kuidas muuta oma ko
www.lukuexpert.ee/turvaline-kodu ▼ [Translate this page](#)

Ka tagauks olgu turvaline. Tagauks ei ole tavaliselt nähtav ja seetõttu on see Sinu kodu turvalisuse seisukohast nõrgim lüli. Paigalda kõikidele välisustele ...



Elu pärast “sündmusi”



HOME ABOUT NSA ACADEMIA BUSINESS CAREERS INFORMATION ASSURANCE RESEARCH PUBLIC INFORMATION CIVIL LIBERTIES

Information Assurance

About IA at NSA
IA Client and Partner Support
IA News
IA Events
IA Mitigation Guidance
IA Academic Outreach
IA Business and Research

IA Programs

Commercial Solutions for Classified Program
Global Information Grid
High Assurance Platform
Inline Media Encryptor
Suite B Cryptography
NSA Mobility Program
National Security Cyber Assistance Program
IA Careers
Contact Information

Home > Information Assurance > Programs > NSA Suite B Cryptography

Cryptography Today

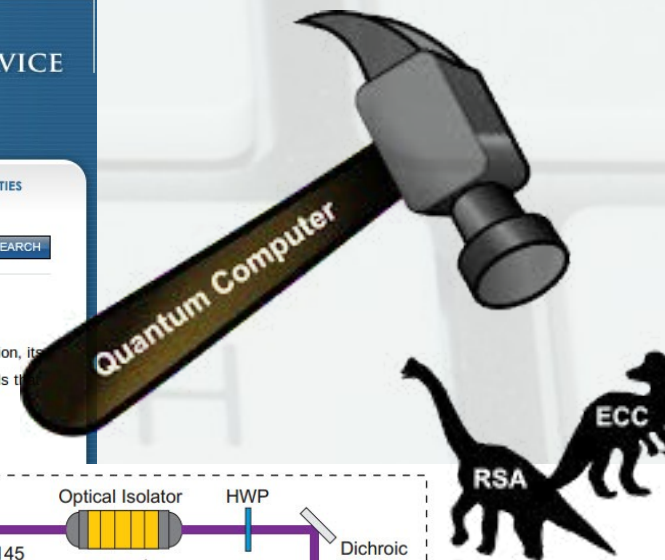
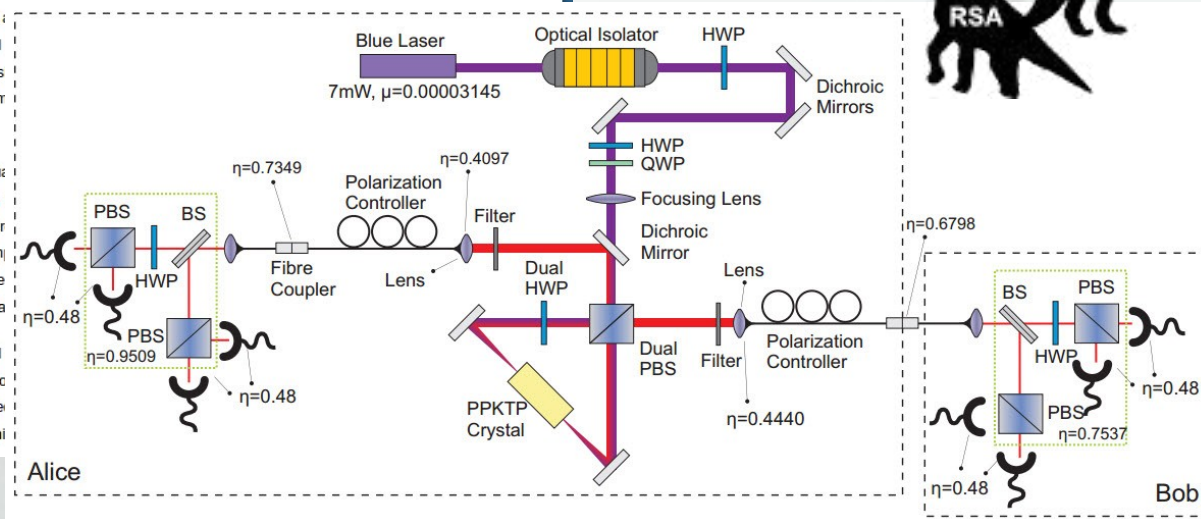
In the current global environment, rapid and secure information sharing is important to protect our Nation, its citizens and its interests. Strong cryptographic algorithms and secure protocol standards are vital tools that contribute to our national security and help address the ubiquitous need for secure, interoperable communications.

Currently, Suite B cryptographic Technology (NIST) and are used protecting classified and unclassified plans for transitioning to quantum

Background

IAD will initiate a transition to quantum experience in deploying Suite B, upcoming transition to quantum against a potential quantum communication standards bodies to ensure there open and transparent manner that

Until this new suite is developed will rely on current algorithms. For B elliptic curve algorithms, we are instead to prepare for the upcoming



Sisuline sõnum?

In August, National Security Agency officials advised US agencies and businesses to prepare for a not-too-distant time when the cryptography protecting virtually all sensitive government and business communications is rendered obsolete by quantum computing. The advisory recommended backing away from plans to deploy elliptic curve cryptography, a form of public key cryptography that the NSA spent the previous 20 years promoting as more secure than the older RSA cryptosystem.

2015-10-23



A RIDDLE WRAPPED IN AN ENIGMA

NEAL KOBLITZ AND ALFRED J. MENEZES

ABSTRACT. In August 2015 the U.S. National Security Agency (NSA) released a major policy statement on the need for post-quantum cryptography (PQC). This announcement will be a great stimulus to the development, standardization, and commercialization of new quantum-safe algorithms. However, certain peculiarities in the wording and timing of the statement have puzzled many people and given rise to much speculation concerning the NSA, elliptic curve cryptography (ECC), and quantum-safe cryptography. Our purpose is to attempt to evaluate some of the theories that have been proposed.

<http://eprint.iacr.org/2015/1018.pdf>

Koblitz/Menezes: 5 teooriat

- The NSA can break PQC.
- The NSA can break RSA.
- The NSA was thinking primarily of government users.
- The NSA believes that RSA-3072 is much more quantum-resistant than ECC-256 and even ECC-384.
- The NSA has a political need to distance itself from ECC.



Meile olulised arengusuunad

- Suurfirmade tehnoloogilised valikud
- Krüptograafia kui inimõigus
- Kvantkrüptograafia-järgne maailm
- Kvaliteetselt universaalne uuendusnupp
- Paanikahalduse parimad praktikad
- Ja meid saab palju! (vähemalt 10 miljonit)



Tähh!

Paar küsimust?!