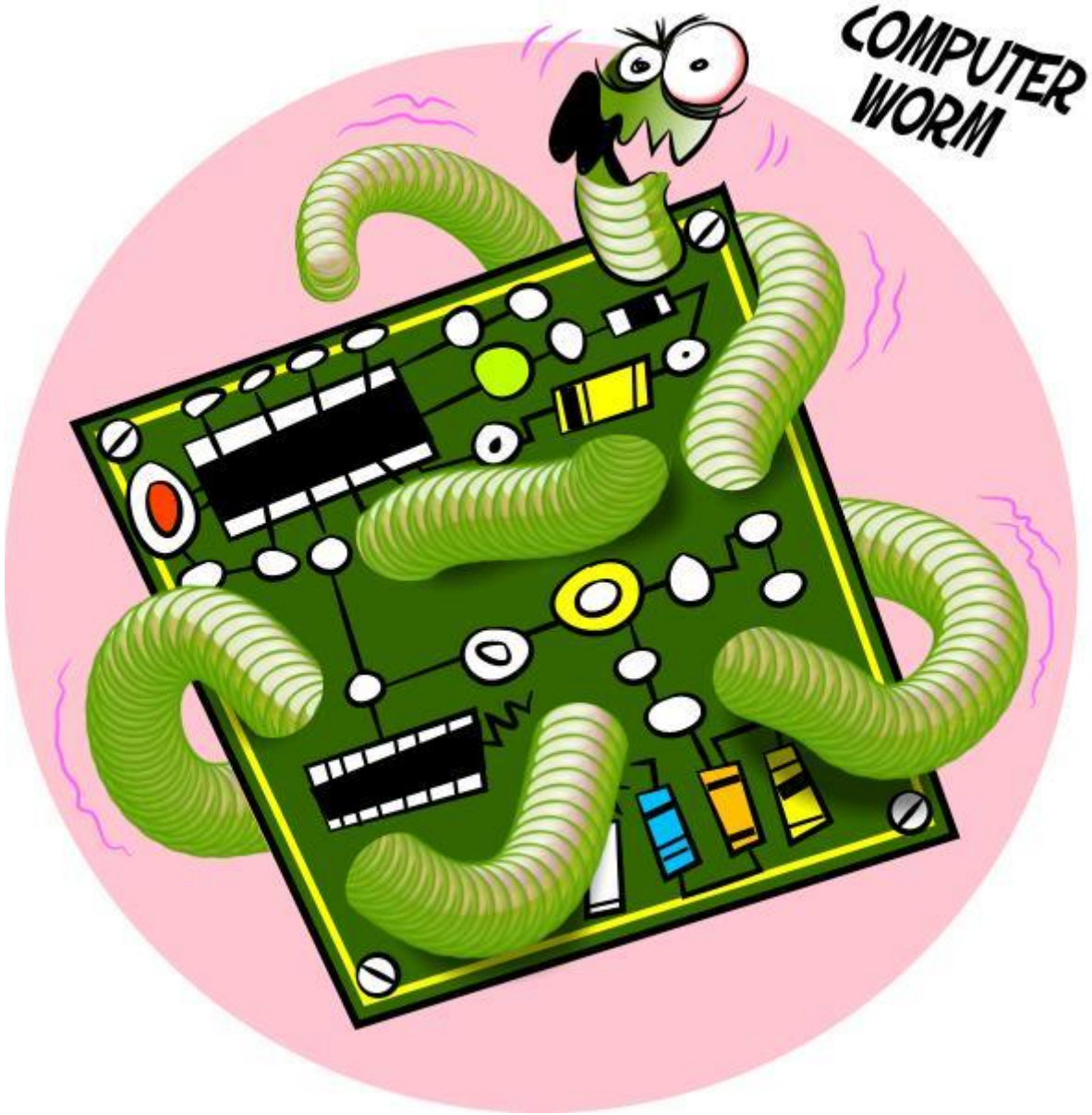
15. Küberturvalisus

Side IRT3930

Ivo Müürsepp

Pahavara

- Viirus
- Uss (*Worm*)
- Troojalane
- Käomuna (*Rootkit*)
- Lunavara (*Ransomware*)



Stuxnet

Foto: http://www.globalsecurity.org/

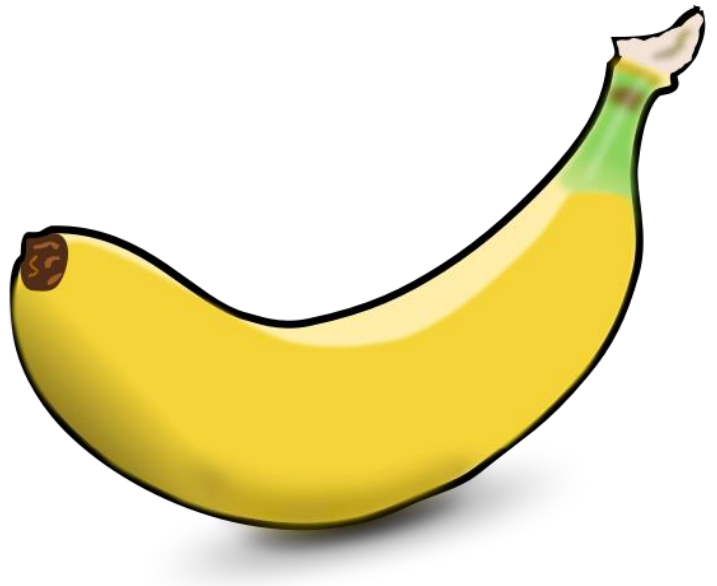
Tagauks

- Sisse ehitatud
- Vead süsteemi ehituses
- Hiljem juurde lisatud
  - Kasutaja poolt
  - Ründaja poolt

Joonis: http://www.witiger.com/ecommerce/sony-rootkit.jpg

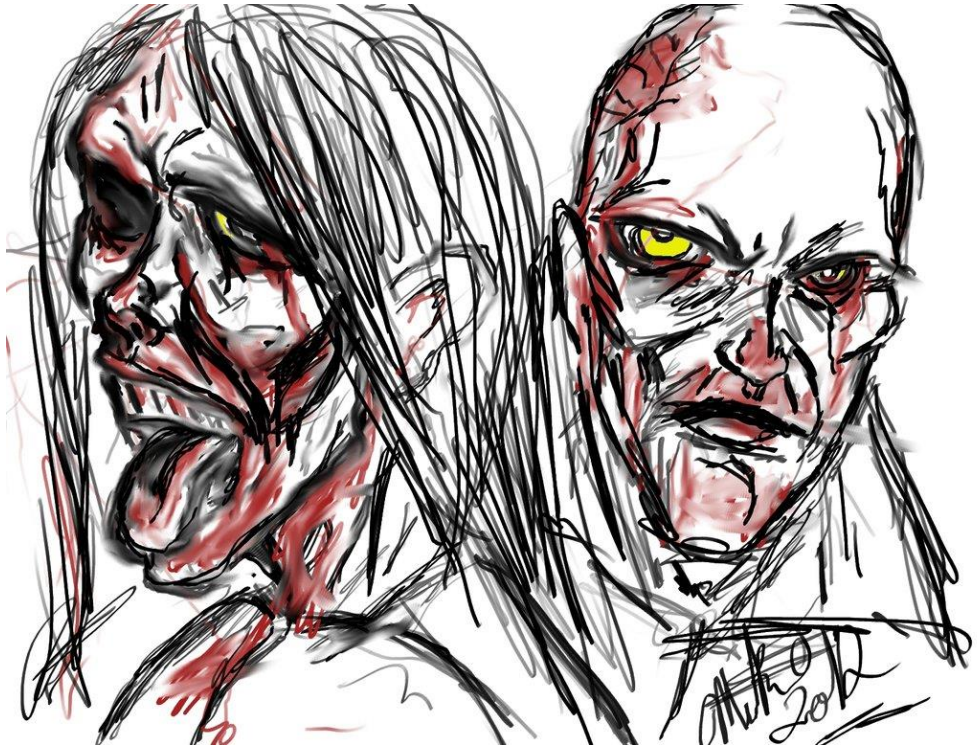
DoS-rünnak (*Denial of Service*)

- Takistamaks sihipärastel kasutajatel juurdepääsu seadmele või võrgule.
- Pingi ujutus (*ping flood*)
- Surmav ping (*Ping of death*)
- SYN ujutus (*SYN flood*)
- Püsiv kahju (*PDoS – Permanent DoS*)
- Banaanirünnak
- „Must faks“
- ZIP-pomm
  - 42.zip 4,5 PB ($4{,}5 \cdot 10^{15}$ B)



Hajutatud DoS rünnak (*DDoS*)

- Zombivõrk (*Botnet*)
- Vabatahtlikud zombid

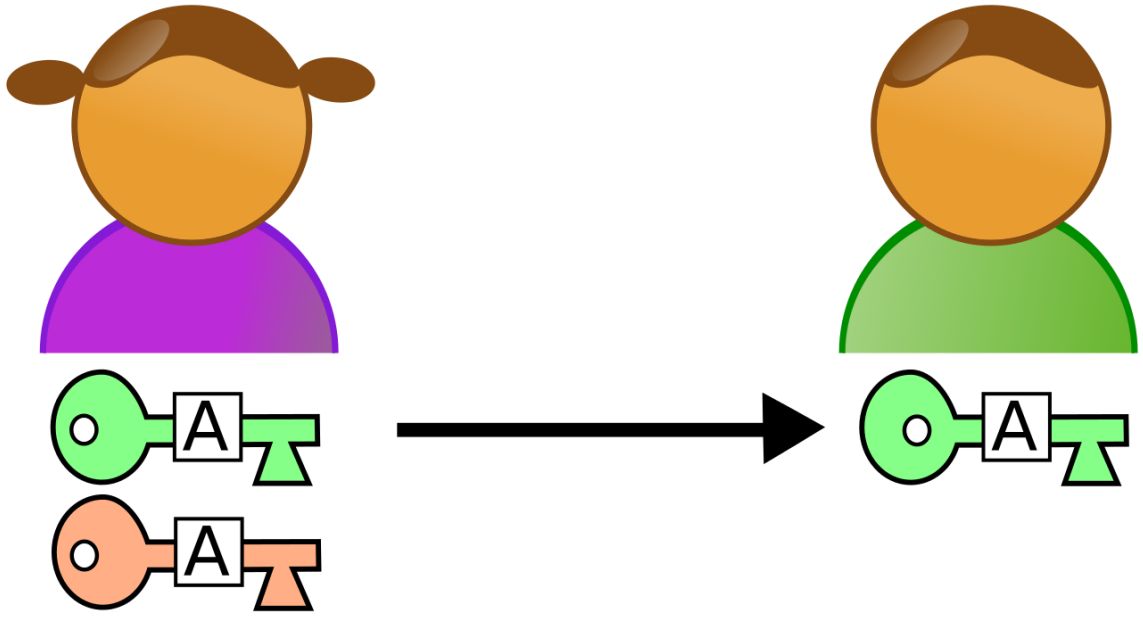


Low Orbit Ion Cannon (*LOIC*)

Joonis: http://gizmodo.com

Krüptograafia

- Andmete salvestamise ja edastamise meetodid, mis tagavad juurdepääsu ainult neile kasutajatele, kellele see on mõeldud.



Asendusšiffer

- Lahtise teksti (*plaintext*) sümbolite asendamine mingi reegli järgi šifertekst (*chipertext*) sümbolitega.
- Lihtsaim näide on nn Caesari- ehk nihkešifer

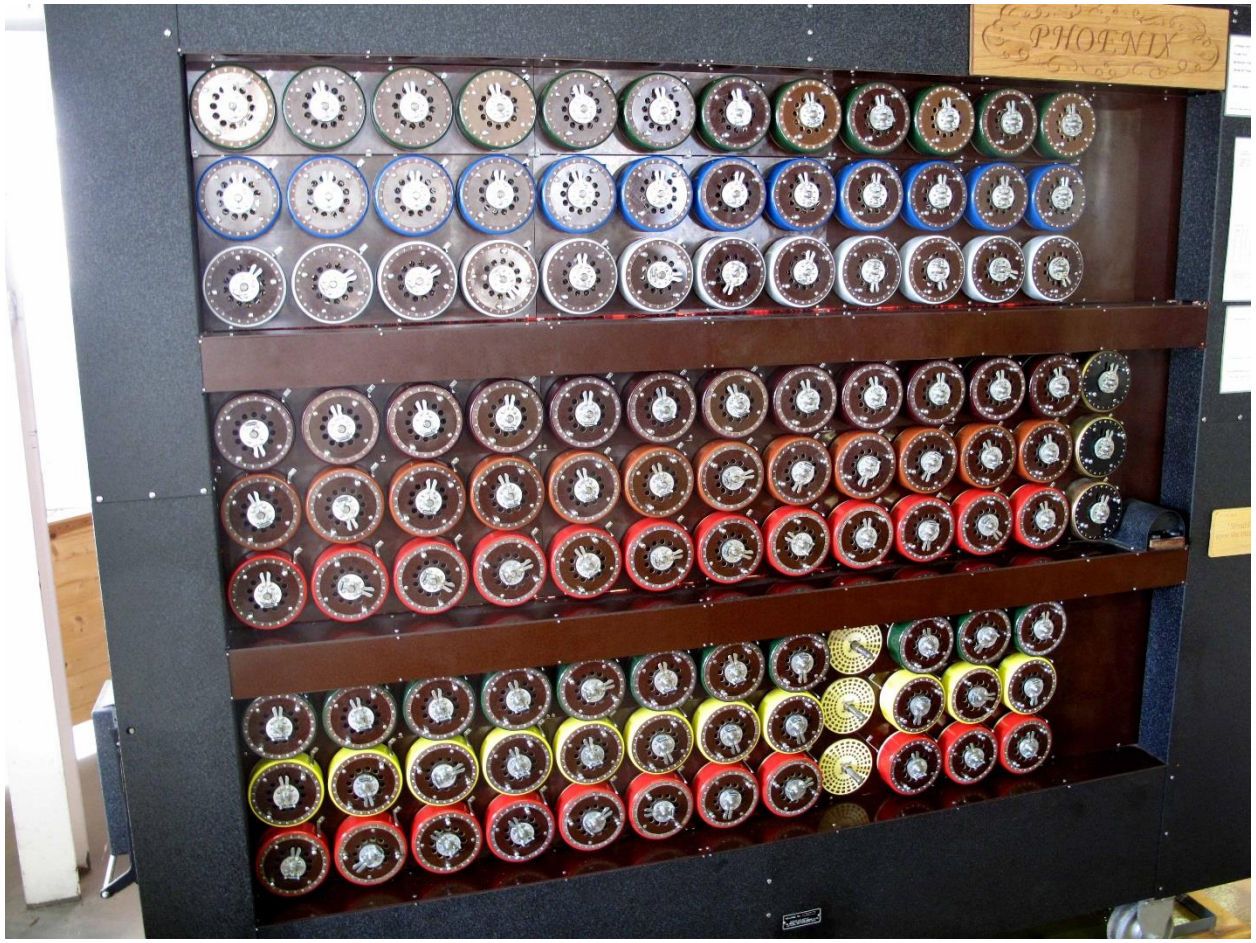
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	Š	Z	Ž	T	U	V	W	Õ	Ä	Ö	Ü	X	Y
Ü	X	Y	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	Š	Z	Ž	T	U	V	W	Õ	Ä	Ö

Sõnum: KUI ARNO ISAGA KOOLIMAJJA JÕUDIS

Šifertekst HZF ÜOKL FPÜDÜ HLLIFJÜGGÜ GUZAFP

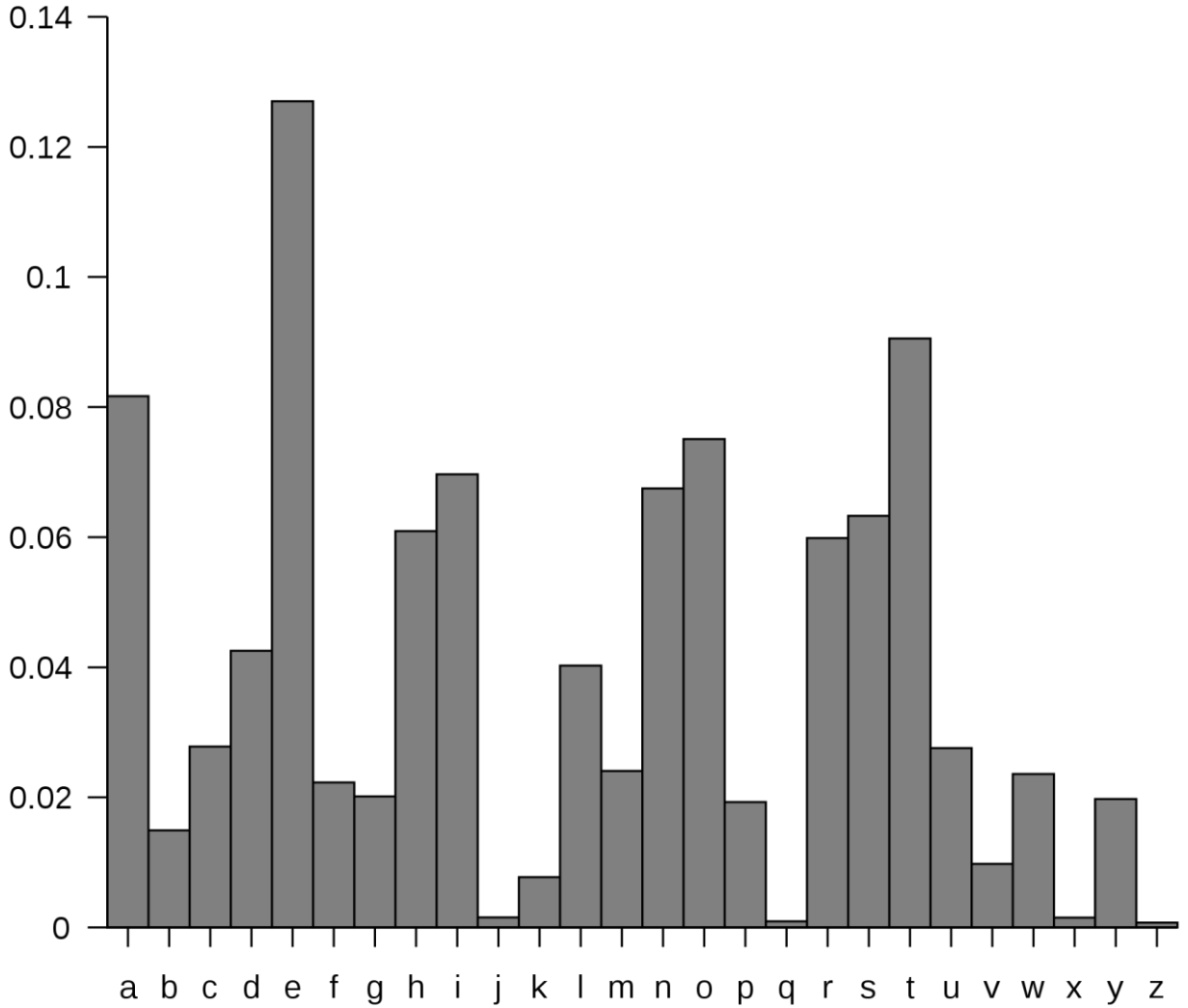
Šifri lahti murdmine

- Krüptoanalüüs
  - Statistilised meetodid
- Toore jõuga lahtimurdmine
  - Arvutusvõimsus
- Kõrvalkanali rünnakud



Joonis: www.wikipedia.org

Ingliskeelse teksti tähtede esinemissagedused



Joonis: www.wikipedia.org

Kerckhoff’i printsiip

„Enemy knows the system“

C. Shannon

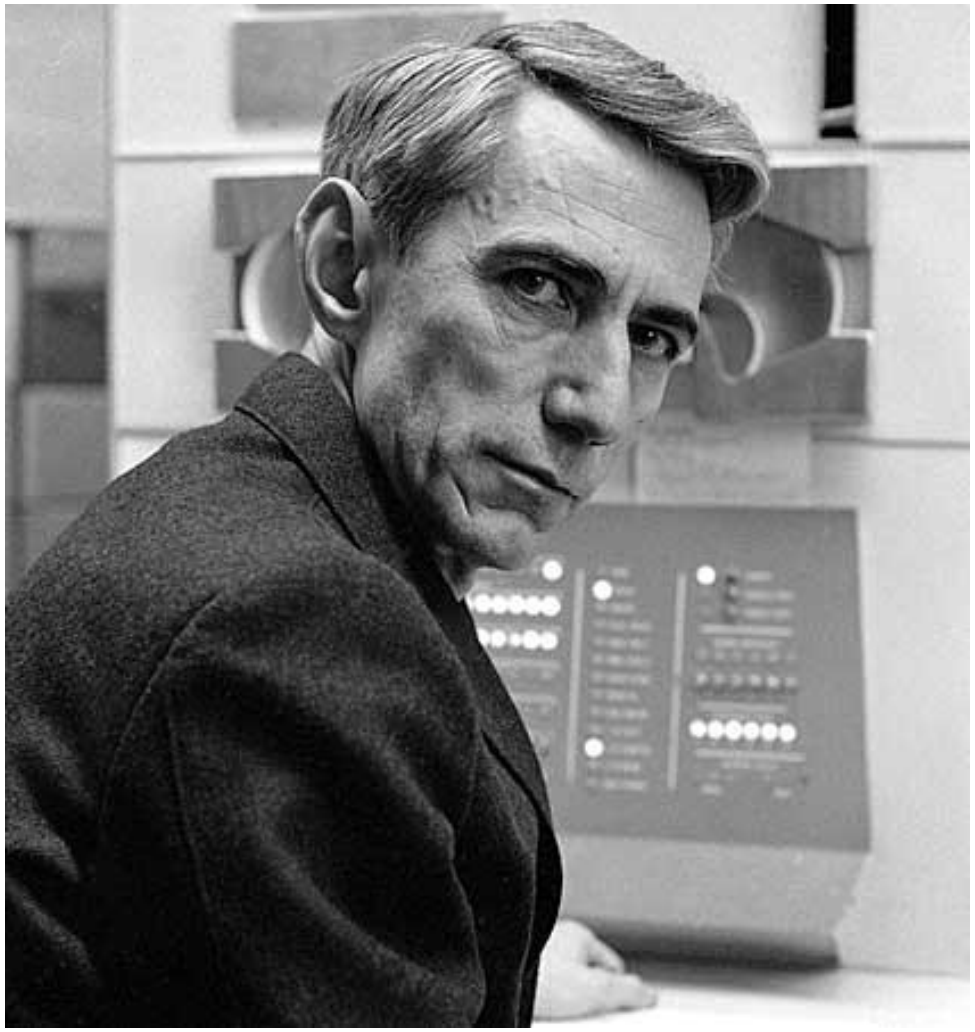
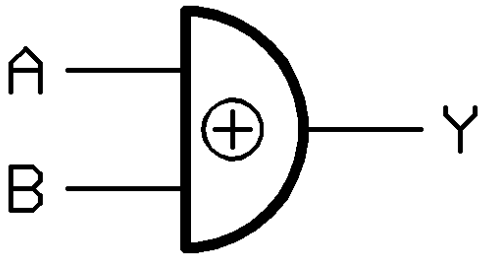


Foto: http://www.mogensjacobsen.dk/showwork.php?pid=16

Ühekordne šiffer

- Ühekordne šiffer (*OTP – One Time Pad*) on õige kasutamise korral lahtimurdmatu.
  - Võti peab olema täiesti juhuslik ja vähemalt sama pikk kui lahtine tekst.
  - Igat võtit võib kasutada ainult korra
  - Võtit tuleb hoida rangelt saladuses
  - Krüpteerimisel liidetakse iga lahtise teksti bitt mooduliga kaks kokku võtmega.



Sümmeetriline Krüpteerimine

- Ajalooline meetod. Kuni eelmise sajandi seitsmekümnendateni ainus viis.
- Krüpteerimiseks ja dekrüpteerimiseks üks ja sama, salajane võti
  - Kuidas võtit turvaliselt jagada?
- *DES – Data Encryption Standard*
  - 56 bitine võti.
  - Kasutuses aastast 1977
  - 1998 aastal murti lahti.
    - 250.000$ maksev seade vähem kui kolme päevaga
  - 3DES
- *AES – Advanced Encryption Standard*
  - Vähemalt 128 bitine võti

Keskmine võtme lahti murdmise aeg

Võtme pikkus [bit]	Võtmete arv	1 võti/µs	10^6 võtit/µs
32	$4{,}3 \cdot 10^9$	35,8 minutit	2,15ms
56	$7{,}2 \cdot 10^{16}$	1142 aastat	10 tundi
128	$3{,}4 \cdot 10^{38}$	$5{,}4 \cdot 10^{24}$ aastat	$5{,}4 \cdot 10^{18}$ aastat
168	$3{,}7 \cdot 10^{50}$	$5{,}9 \cdot 10^{36}$ aastat	$5{,}9 \cdot 10^{30}$ aastat

Salajase võtme avalik jagamine

- Diffie-Hellman'i võtmevahetus
- Vahetuse aluseks on avalikud arvud g ja p, kus g on algjuur (*primitiive root*) mooduliga p.
  - Näiteks $p = 25$ ja $g = 8$
- Kumbki osapool valib juhusliku salajase täisarvu
  - Alice: $a = 5$
  - Bob: $b = 4$
- Kumbki osapool arvutab avalikult edastatavad suurused
  - Alice: $A = g^a \bmod(p) = 8^5 \bmod(25) = 18$
  - Bob: $B = g^b \bmod(p) = 8^4 \bmod(25) = 21$

Salajase võtme avalik jagamine

- Kumbki osapool saab teiselt avaliult edastatud suuruse (A või B), mille põhjal leitakse **ühine salajane võti**, mida kasutatakse edasise side krüpteerimiseks.
  - Alice saab $B = 21$ ja arvutab $B^a \bmod(p) = g^{ba} \bmod(p) = 21^5 \bmod(25) = \mathbf{1}$
  - Bob saab $A = 18$ ja arvutab $A^b \bmod(p) = g^{ab} \bmod(p) = 18^4 \bmod(25) = \mathbf{1}$
- Mooduliga astendamine on isegi suurte arvude puhul kiirelt realiseeritav tehe.
- Juhul kui p on vähemalt 600 kohaline algarv on p,g, A ja B teades a ja b leidmine mõistliku aja jooksul üle jõu käiv probleem (*discrete logarithm problem*).

Autentimine

- Kaitse aktiivse rünnaku, spoofimise ja andmete muutmise vastu.
- Kellelt on andmed pärit? Kas tegelik allikas on see, kes ta väidab end olevat?
- Kas andmeid on ülekande käigus kolmandate osapoolte poolt muudetud?

Avaliku võtmega krüpteerimine

- Asümmeetriline krüpteerimine
- Kaks eraldi võtit:
  - Salajane – teada ainult omanikule
  - Avalik – teada teistele osapooltele
  - Puudub vajadus salajase võtme turvaliseks jagamiseks
- Digitaalne allkirjastamine
- RSA algoritm (.ddoc)
- ECDSA (.bdoc)

Joonis: https://www.politsei.ee/

Rivest–Shamir–Adleman (RSA)

- Põhineb suurtel algarvudel
  - Suurim teadaolev algarv (käesoleva kuu seisuga): $2^{74,207,281} - 1$
  - Selle arvu pikkus on 22,338,618 kümnendkohta
  - Tegemist on Mersenne algarvuga, avaldub kujul $M_n = 2^n-1$
- Vali kaks juhusliku, erinevat algarvu p ja q
  - Näiteks $p = 61$ ja $q = 53$
- Arvuta nende korrutis $n = p \cdot q$
  - $n = 61 \cdot 53 = 3233$
  - n - pikkus bittides on võtme pikkuseks
- Leia arvude $(p-1)$ ja $(q-1)$ vähim ühiskordne $\lambda(n) = \text{vük}(p-1, q-1)$
  - $\lambda(3233) = \text{vük}(60, 52) = 780$

RSA

- Väli täisarv e vahemikust $1 < e < \lambda(n)$, selliselt et e ja $\varphi(n)$ suurim ühiskordaja oleks 1 (kaasalgarvud).
  - Kui e on algarv on vaja ainult kontrollida, et $\lambda(n)$ ei oleks e täisarvkordne
  - Näiteks valime $e = 17$
- Leia selline täisarv d, et $d \cdot e \bmod(\lambda(n)) = 1$
  - Meie näites $d = 413$
  - Kontroll $d \cdot e = 17 \cdot 413 = 7021 = 9 \cdot 780 + 1 = 9 \cdot \lambda(n) + 1$
- Avalik võti koosneb n ja e –st: $PU = \{n, e\}$
  - $PU = \{3233, 17\}$

RSA

- Salajane võti koosneb n ja d-st: $PR = \{n, d\}$
  - $PR = \{3233, 413\}$
- Krüpteerimine: $c(m) = m^e \bmod(n)$
  - Näiteks olgu avalik tekst $m = 65$
  - $c(m) = 65^{17} \bmod(3233) = 2790$
- Dekrüpteerimine: $m(c) = c^d \bmod(n)$
  - $m(c) = 2790^{413} \bmod(3233) = 65$

Juurdepääs

- Pealtkuulamine
  - *Van Eck phreaking*
- Spoofimine (*spoofing*)
- Kasutusõiguste suurendamine
- Õngitsemine (*phishing*)
  - Nigeeria printsi kirjad
  - www.swedbank.naide.ee
  - www.swedbank.ee
- Klikkide kaaperdamine (*clickjacking*)

Tere sõber.

Ma olen Teiega küsida teie abi selle ärisaladust ettepaneku täieliku rahalise (£ 11,500,000.00) kasu meile mõlemale.

Ma annan teile põhjaliku detail niipea kui saan sõna sinult. Kui saame olla ühel, saatke mulle oma vastus näitab teie huvi on e-posti alla, et saaksime alustada selle mõttekäik.

Märkus: Ma ei ole väga hea eesti keele kõnelejaid; kui sa ei räägi, kirjutada ja mõista inglise keelt, siis palun andke mulle teada, kui see on parem meie suhtlemine.

Südamlikud tervitused,
Sir. Jon Cunliffe
Asekuberner,
finantsstabiilsuse
Bank of England.
Tel: + 44 (0) 701 004 6359
E-mail: j_cunliffe0@aol.co.uk

Levinumad paroolid 2014

- **123456**
- **password**
- **12345**
- **12345678**
- **qwerty**
- **123456789**
- **1234**
- **baseball**
- **dragon**
- **football**

Vastumeetmed

- Tulemüür
  - Paketifilter (OSI 1.-3. kiht)
    - Tumedad aadressid e marslased
  - Olekupõhine (*statefull*) (OSI 4. kiht)
  - Rakenduskihi
- Proksi (puhver)
- Võrguaadressi translaatorid (*NAT*)

Virtuaalne privaatvõrk VPN

- Asutuse sisevõrgus olevate ressursside jaotamine
  - Kaugtöötajatega
  - Asutuse, geograafiliselt eraldiseisvate, filiaalidega
- Kasutaja privaatsuse tagamine
- Luuakse turvaline, krüpteeritud kanal, üle avaliku võrgu – **tunnel**.
  - Autentimine
  - Ligipääsu kontroll
  - Andmete kaitsmine (krüpteerimine)
  - Andmete terviklikkuse tagamine

Virtuaalne tunnel

- Kasutusel mitmeid protokolle:
  - Ipsec
  - PPTP (*Point-to Point Tunneling Protocol*)
  - L2TP (*Layer 2 Tunneling Protocol*)
  - …

AH - Audentification Header

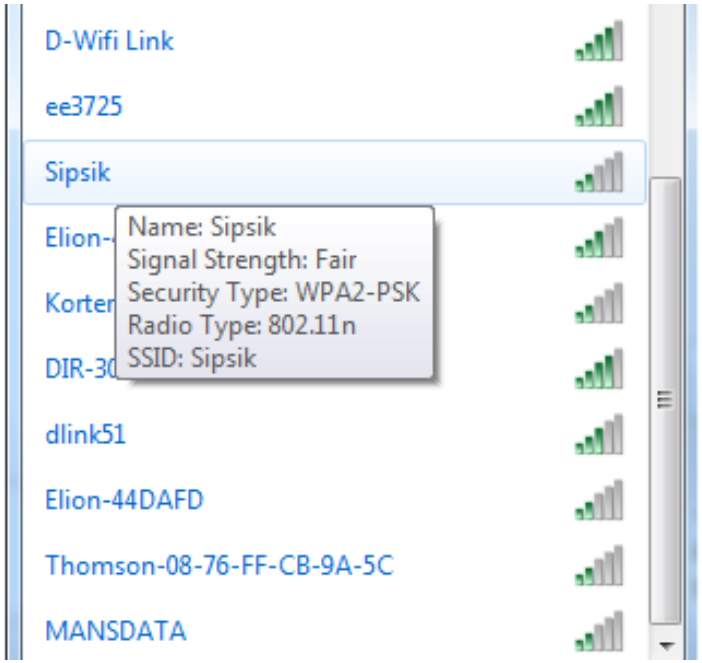
	okt	0								1								2								3							
okt	bitt	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Järgmine päis								*AH* Päise pikkus								Reserveeritud															
4	32	Turvaparameetrite indeks (*SPI*)																															
8	64	Järjekorranumber																															
12	96	Audentimisinformatsioon																															
…	…																																
….	…																																

ESP - Encapsulating Security Payload

	okt	0								1								2								3							
okt	bitt	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Turvaparameetrite indeks (*SPI*)																															
4	32	Järjekorranumber																															
8	64	Andmed																															
12	96																																
16	128	Täide (vajadusel)																Täite pikkus								Järgmine päis							
20	160	Audentimisinformatsioon																															

IEEE 802.11

- Turvalisus
- SSID- *Service Set IDentifier*
- WEP – Wired Equivalent Privacy
  - Caffe Latte Attack
- WPA – WiFi Protected Access
  - WPA2
  - PSK – Pre Shared Key



Ülesanded

- Ühekordse šifriga (OTP) krüpteeritud tekst (16-bitine) on kuueteistkümnendarvuna kujul 0xA257. Leia algne lahtine tekst (*plaintext*), kui võti on 0x1CBD.
- Kui palju aega kuluks 40 bitise võtme toore jõuga lahti murdmiseks kui selleks kasutatava arvuti jõudlus on $2{,}5 \cdot 10^9$ võtit sekundis?

Loe lisaks

- William Stallings. **Data and Computer Communications.** Kaheksas trükk. Peatükk 21 – **Network Security.**
- Erkki Laaneoks. **Sissejuhatus võrgutehnoloogiasse**. 18.2 **VPN**