

Krüptograafia ajalugu

Erika Matsak

Vana-Egiptus

- Ligi 4000 aastat tagasi (1900 eKr) Meneth-Hufu linnas, Niiluse jõe ääres, joonistas üks Egiptuse kirjatundja hieroglüüfid, mis kirjeldasid tema isanda Khnumhotep'i elulugu. See lugu ei olnud šifreeritud, ainult kohati olid hieroglüüfid asendatud teiste sümbolitega. Nende asenduste eesmärgiks oli pöörata tähelepanu nimetatud tekstile



Vana-Egiptus



Vana India

- Vana India riigi juhtimise traktaadis (300 eKr) on kirjas soovitus luurejuhile, et ta jagaks oma käske agentidele salakeeles.



Lihtne kodeerimisviis: Atbash (VI eKr)

- Kodeerimisviis, mis asendab olemasolevad märgid teiste märkidega
- Antud juhul asendatakse märk, mille positsioon tähestikus on i , selle märgiga, mille positsioon tähestikus on $n-i+1$, kus n on märkide arv tähesikus.

1	2	3	4	5	6	7	8	9	10	11	12
A	b	c	d	e	f	g	h	i	j	k	l

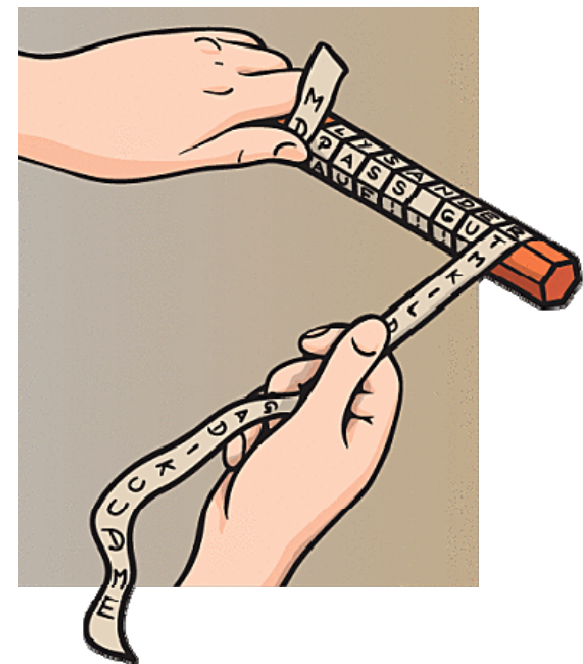
13	14	15	16	17	18	19	20	21	22	23	24	25	26
m	n	o	p	q	r	s	t	u	v	w	x	y	z

Skytale (V eKr)

- Vana Sparta kood – olemasolevate märkide järjekorra muutmise (permutatsioon) kood.

Help me I am under attack

	H	E	L	P	M	
	E	I	A	M	U	
	N	D	E	R	A	
	T	T	A	C	K	



<http://www.youtube.com/watch?v=GEICkI98EP8>

Polybiose ruut (Vana-Kreeka)

II sajand eKr

- Tähed kirjutatakse 5x5 ruutu. Kuna Kreeka tähestikus on 24 sümbolit, siis jäi üks lahter tühjaks. Optilise telegraafi abil edastati sümboleid vastava rea numbri ja tulba numbri abil.
- Esimene süsteem, mis “pakkis” tähestikku ning mingil määral on kahendsüsteemi prototüüp

	1	2	3	4	5
1	Α	Β	Γ	Δ	Ε
2	Ζ	Η	Θ	Ι	Κ
3	Λ	Μ	Ν	Ξ	Ο
4	Π	Ρ	Σ	Τ	Υ
5	Φ	Χ	Ψ	Ω	

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

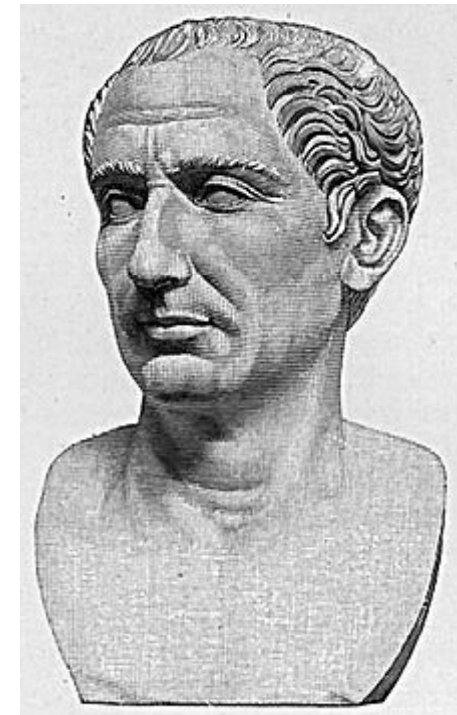
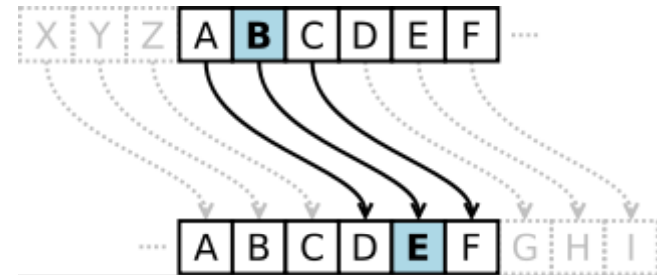
Sõna “INFO” kodeeritud kujul:
24332134

Caesari šiffer (50a eKr)

- Šifreerimise käigus iga täht asendatakse teise tähega, mis paikneb tähestikus konkreetse arvu n nihkega. Caesar kasutas sellist šifrit oma kirjavahetuses

$$E_n(x) = (x + n) \pmod{26}.$$

$$D_n(x) = (x - n) \pmod{26}.$$



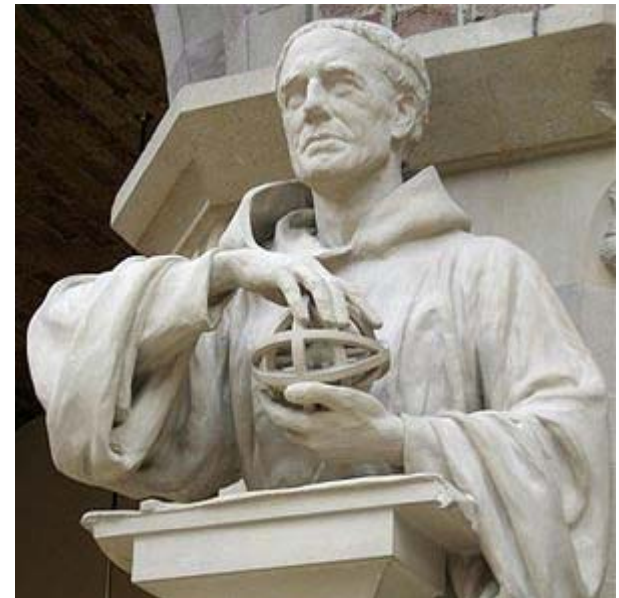
Araabia krüptograafia, VIII sajand

- Al-Khalil kasutab “standartseid” fraase kui krüpteerimisvõtit (790 a p. Kr). Ta tegi ettepaneku, et olgu näiteks esimeseks fraasiks “Allahi nimel”, ning selle fraasi abil oli võimalik dekrüpteerida ülejäänud teksti



Roger Bacon (c. 1214–1294)

- Esimene Euroopas ilmunud krüptograafia pühendatud raamat, mille autoriks oli Roger Bacon, «*Epistola Fratris Rog. Baconis, de secretis operibus artis et naturae et nullitate magiae*», käsitles muu hulgas 7 erinevat krüpteerimisviisi



Statue of Roger Bacon in the Oxford University Museum

Šifreerimise disk (XV sajand)

- Leon Battista Alberti “De Cifris” 1467.
- Väline disk on fikseeritud (mitte liikuv) ning on jaotatud 24ks sektoriks (20 ladina tähestiku tähte ja numbrid 1,2,3,4). Sisemine disk on liikuv ning on samuti jagatud 24 sektoriks (24 tähte mitte-tähestikulises järjekorras).
- Osapooled pidid leppima kokku milline tähtede järjekord on sisemisel diskil ning kuidas see peab olema positsioneeritud (“starditähe” asukoht!). Samuti peab olema kokkulepe, et mitme šifreeritud sõna järel toimub “võtme” vahetus, ehk millal keeratakse disk ühe positsiooni võrra edasi
- dunaamiline šifreerimine – kasutab mitut tähestikku (polyalphabetic substitution)



(February 18, 1404 – April 20, 1472)

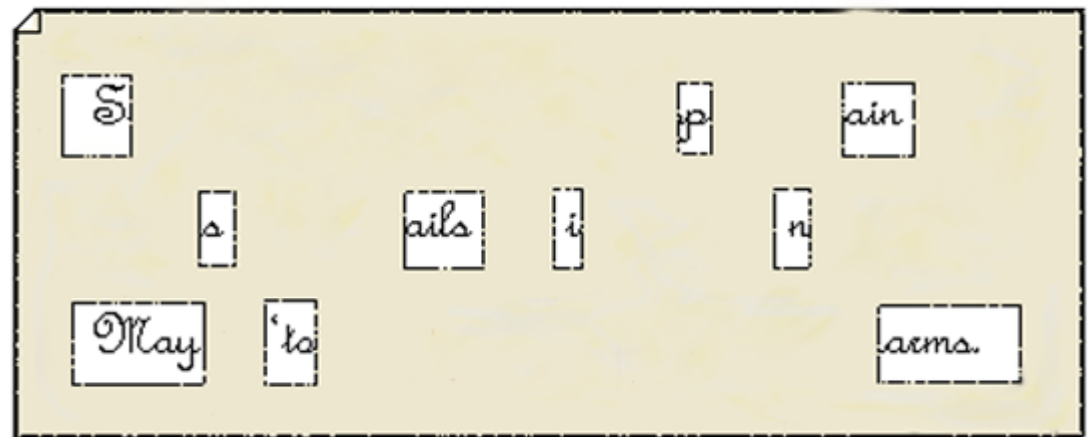
Cardano võre

- Kodeerimis-dekodeerimis vahend, mis kujutas endast kaarti, milles mõned lahtrid olid välja lõigatud. Salatekst kirjutati nendesse lahtritesse, pärast täideti ülejäänud ruum sobivat, tähendust omava tekstiga.



(24 September 1501 – 21 September 1576)
Itaalia matemaatik, füüsik ja astroloog

*Sir John regards you well and spekes again that
all as rightly 'sails him is yours now and ever.
May he 'tore for past d'lays with many charms.*





Blaise de Vigenère

- Antud šiffer kombineerib mitut Caesari šifrit erineva sammuga
- Tabelis esimesele reale kirjutatakse tähestik (26 tähte), siis iga järgmisele reale tähestik, mis on nihutatud mõne sammu võrra. Kokku saadakse 26 erinevat šifrit. Šifreerimise etappidel valitakse erinevad “read” vastavalt võtmele

$$C_i \equiv (P_i + K_i) \pmod{26}$$

$$P_i \equiv (C_i - K_i) \pmod{26}$$

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

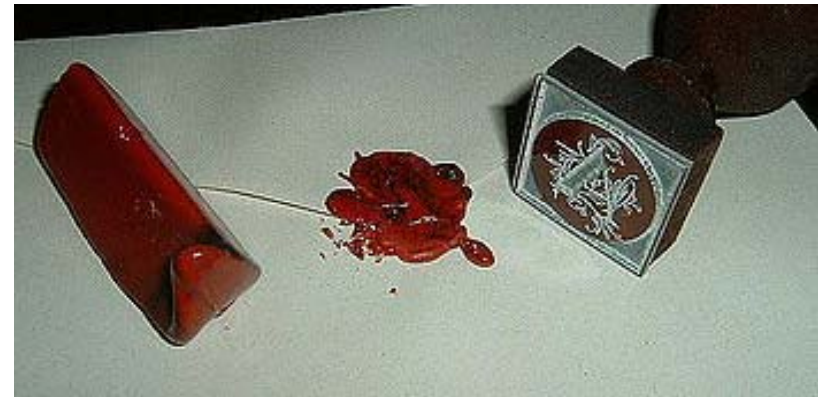
Olgu algtekstiks ATTACKATDAWN ning võtmesõnaks LEMON.

Kõigepealt “suurendatakse” võtmesõna algteksti pikkuseni: LEMONLEMONLE.

Krüpteeritud: LXFOPVEFRNHR.

“Must kabinet” (*Cabinet Noir*)

- Asutus, mis tegeles kirjade “ülelugemisega” ja nende dešifreerimisega
- Prantsuse kuningas Henry IV avas posti teenistuse «Poste aux Lettres», mille ülesandeks oli avada, lugeda ning uuesti pitseerida kirjad, eesmärgiga korjata infot rahva meeleolu kohta
- Esimene “Must kabinet” alustas oma tööd 1668a
 - Inglismaa, Austria, Püha Saksa-Rooma keisririik, Holland, Taani, Venemaa.
- 1911 a entsüklopeedias “Britannica” on kirjutatud, et “Mustad kabinetid” enam ei eksisteeri
- 1921a- uus ajastu Nõukogude liidus



Antoine Rossignol (1600–1682)

Matemaatilise krüptograafia suunas

- 1824 Jean-François Champollion, «Précis du système hiéroglyphique» ("Hieroglüüfide süsteemi selgitus")
- Püüdis dešifreerida egiptuse hieroglüüf-kirja. Rosetta kivi ja teiste raidkirjade abil dešifreeris palju hieroglüüfe.



(23 detsember 1790
— 4 märts 1832)

Matemaatilise krüptograafia suunas

- 1863 Friedrich Kasiski (29 November 1805–22 May 1881) publitseeris meetodi ("Secret writing and the Art of Deciphering"), mille abil oli võimalik dešifreerida kõiki selle ajastu šifreid.
 - Saada aru kas tegu on monotähestikuga või polütähestikuga
 - Kirjutada välja korduvaid osi ning vaadata nende asukohta
 - Detailne analüüs näiteks 6 erineva tähestiku juures

<http://www.ics.uci.edu/~gts/268/vigenere.html>

Matemaatilise krüptograafia suunas

- 1883 Auguste Kerckhoffs “Sõjaline krüptograafia”, milles formuleeriti vastused küsimustele, mis said aktuaalseks alles XX sajandil.
- Süsteemses vormis esitas nõudmised krüptosüsteemile, samuti tõstis esile, kui oluline on veenduda, et šiffer on “kindel”:
 - Šiffer peab olema murdmatu
 - Võti peab olema lihtsasti meelde jääv ning kergesti muudetav
 - Šifreerimise abivahend peab olema lihtsasti transporditav
 - Šifreeritud teksti peab saama edastama telegraafi abil
 - Šifreerimise abivahend peab olema lihtsasti kasutatav ning mitte nõudma erilist haridust



(19 January 1835 –
9 August 1903)



Matemaatilise krüptograafia suunas

- 1918, William Frederick Friedman
«Index of Coincedence and Its Applications in Cryptography»
- Võttis kasutusele terminid
krüptoloogia ja krüptoanalüüs
- Kolme krüptoloogia õpiku autor
- Üheksa krüptomasina looja



24 september 1891 –
12 november 1969

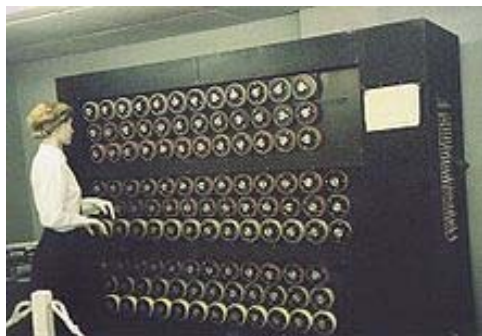
Krüpteerimismasin Enigma

- Portatiivne šifreerimismasin. Loodud aastal 1930 Saksamaal
- Kasutati nii kommertseesmärkidel kui ka sõjalistes ja munitsipaal-asutustes. Laiemat kasutust leidis Sakslastel teise maailma sõda ajal.
- Oli toodetud ligikaudu 100 000 masinat
- $26 \times 26 \times 26 = 17\,576$ erinevat substitutsiooni



<http://www.youtube.com/watch?v=DnBsndE1lkA>

<http://www.youtube.com/watch?v=yKJueRXgWqU&feature=related>



Turing Bombe

- Dešifreerimise masin
- “Bombe” prototüüp oli loodud poola krüptograafi Marian Rejewski poolt enne II Maailmasõda
- Inglismaal jätkati tööd Bletchley pargis Alan Turingi loodud teoreetiliste aluste põhjal
- Esimene “Bombe” masin alustas tööd 18 märts 1940
- Koosnes 108st pöörlevast elektromagnetilisest trumlist ning teistes abistavatest mehhanismidest

<http://www.youtube.com/watch?v=QWAPzkirR3Q>

<http://www.bletchleypark.org.uk/> ning

Bletchley Park Tour - Part 1 :

<http://www.youtube.com/watch?v=ZmMFp2FQPsY>



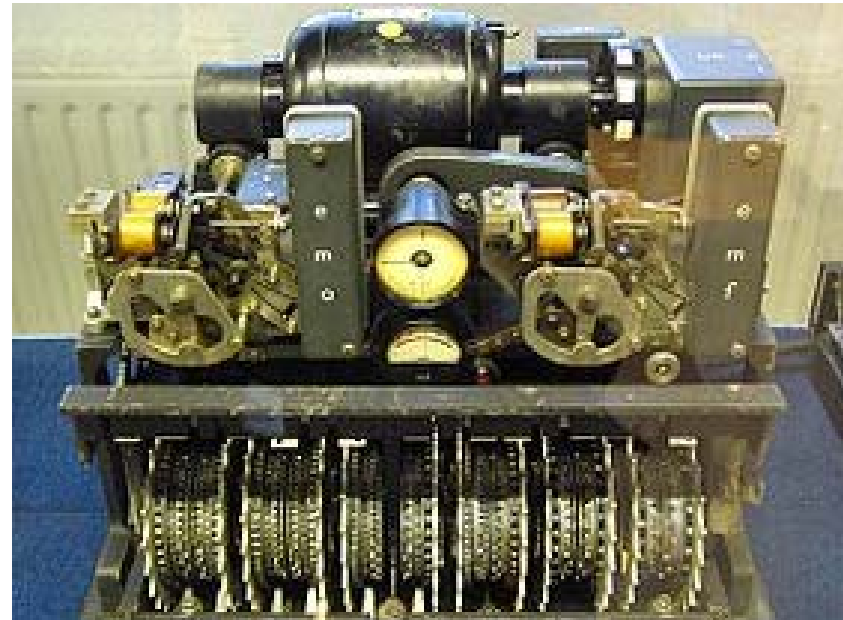
(M. Rejewski 16. August 1905 – 13. Veebruar 1980)



(A. Turing 23. juuni 1912 – 7. juuni 1954)

Lorenz-i masin

- Lorenz-Chiffre, Schlüsselzusatz; Lorenz SZ 40 и SZ 42
- 1940 a alguses oli esimest korda fikseeritud Inglismaa vastava üksuse poolt, kes kuulas eetris võimalikku luureinfot.
- Murdmatu kood



LETTERS		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	CARRIAGE RETURN	LINE FEED	LETTERS	FIGURES	SPACE	LETTERS NOT USED		
FIGURES		-	?	*	W A L K Y O U	3	%	@	£	8	DEL	()	.	,	9	0	1	4	†	5	7	=	2	/	6	+	LINE	FEED	LETTERS	FIGURES	SPACE	LETTERS NOT USED		
CODE ELEMENTS	1	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	
	2	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	
	3	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
	4	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
	5	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•

The Baudot Code

<http://www.youtube.com/watch?v=69uSSXzImMY>

Colossus

- Esimene programmeeritav “arvuti” maailmas (jaanuar 1943)
- Kasutati Lorenzi masinal kodeeritud kirjade dešifreerimiseks
- 30 augustil 1941 tegi saksa operaator vea, mis andis võimaluse dešifreerimiseks



Traditsioonilise (arvutieelse) krüptograafia lõpp

<http://www.youtube.com/watch?v=ynlyzTluEag>