Matematika skrivnostnih sporočil

Ademir Hujdurović (Univerza na Primorskem, UP FAMNIT)

16.11.2016

Kriptografija

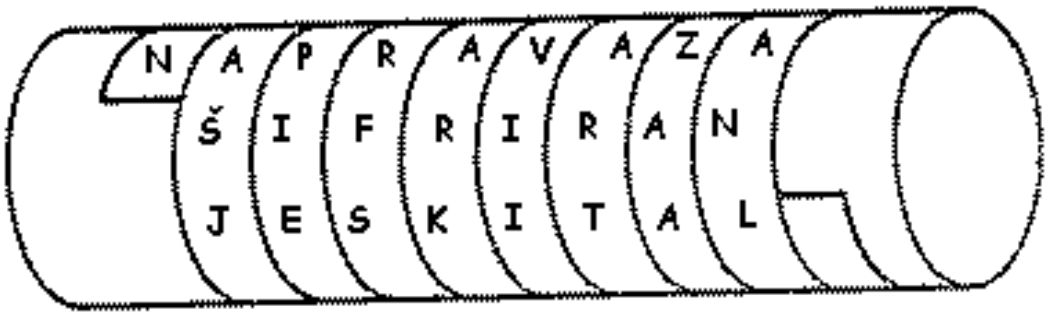
Znanstvena disciplina ki proučuje teoretične in praktične vidike skrivanja sporočil se imenuje kriptografija.
Povezuje področja matematike, računalništva in elektrotehnike.

Kriptografija

Začetki uporabe kriptografije segajo v čase pred našim štetjem. Razvitih je bilo nešteto načinov za zakrivanje sporočil. Prestrezanje sporočil ni bilo v navadi samo v vojnih časih, predvsem prestrezanje diplomatske pošte je bila običajna praksa. Na dvorih so obstajale "črne sobe", kjer so poskušali razvozlati prestrežena in prepisana sporočila.

Skital

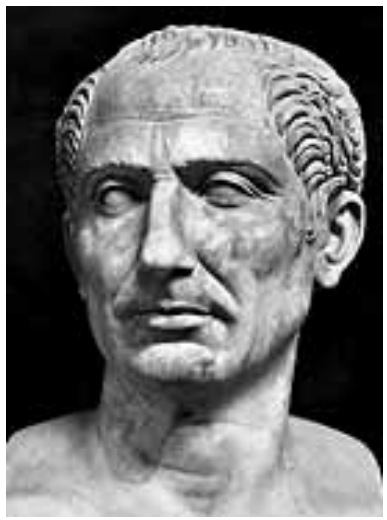
Špartanci so že v 5. stoletju pr.n.št. pošiljali skrivnostna sporočila. Za šifriranje sporočil so vporabljali napravo imenovano skital (ang: scytale). Na valj so navili ozek trak in sporočilo napisali pravokotno na smer traku. Poslali so odvit trak, tako da je sporočilo na videz bilo množica nesmislenih besed. Naslovnik pa je moral imeti valj enakega premera, da bi lahko prebral sporočilo.



Slika: Skital

Cezarjeva šifra

Cezarjeva (ali pomična) šifra je dobila ime po znanem rimskem cesarju Juliju Cezarju, ki jo je uporabljal za pošiljanje vojaških sporočil. Za postopek šifriranja najprej rabimo neko naravno število n ki ga bomo vporabljali kot ključ. Cezar je najbolj pogosto vporabljal vrednost $n = 3$. Potem vsako črko besedila ki ga želimo šifrirati zamenjamo s črko n mest naprej v abecedi.



Slika: Julij Cezar, 102-100 pr. n. št. - 44 pr. n. št.

Cezarjeva šifra

Zgled: Zakodirajmo besedo "ŠIFRA", s ključem $n = 3$.

Cezarjeva šifra

Zgled: Zakodirajmo besedo "ŠIFRA", s ključem $n = 3$.
Rešitev: VLITČ.

Cezarjeva šifra

Zgled: Zakodirajmo besedo "ŠIFRA", s ključem $n = 3$.
Rešitev: VLITČ.
Kako pa poteka postopek dešifriranja?

Cezarjeva šifra

Zgled: Zakodirajmo besedo "ŠIFRA", s ključem $n = 3$.
Rešitev: VLITČ.
Kako pa poteka postopek dešifriranja?
Vsako črko šifriranega besedila zamenjamo s črko ki stoji n mest pred izbrano črko.

Cezarjeva šifra

Zgled: Zakodirajmo besedo "ŠIFRA", s ključem $n = 3$.
Rešitev: VLITČ.
Kako pa poteka postopek dešifriranja?
Vsako črko šifriranega besedila zamenjamo s črko ki stoji n mest pred izbrano črko.
Zgled: Dešifriraj besedilo "Nbufnbujlb kf lvm", če je za šifriranje vporabljena Cezarjeva šifra s ključem $n = 1$.

Kongruence

Kako pa navedeni postopek opišemo bolj v matematičnem jeziku?

Kongruence

Kako pa navedeni postopek opišemo bolj v matematičnem jeziku?
Kongruence: Naj bosta a in b celi števili in m naravno število.
Potem je $a \equiv b \pmod{m}$ natanko takrat ko je $a - b$ deljivo z m.

Kako pa navedeni postopek opišemo bolj v matematičnem jeziku?
Kongruence: Naj bosta a in b celi števili in m naravno število.
Potem je $a \equiv b \pmod{m}$ natanko takrat ko je $a - b$ deljivo z m.

Zgled: Katere izmed nasljednjih trditev so pravilne:

1. $5 \equiv 1 \pmod{2}$;
2. $7 \equiv 3 \pmod{5}$;
3. $2016 \equiv 6 \pmod{10}$;
4. $13 \equiv 18 \pmod{5}$.

Kongruence

Kako pa navedeni postopek opišemo bolj v matematičnem jeziku?
Kongruence: Naj bosta a in b celi števili in m naravno število.
Potem je $a \equiv b \pmod{m}$ natanko takrat ko je $a - b$ deljivo z m.

Zgled: Katere izmed nasljednjih trditev so pravilne:

1. $5 \equiv 1 \pmod{2}$;
2. $7 \equiv 3 \pmod{5}$;
3. $2016 \equiv 6 \pmod{10}$;
4. $13 \equiv 18 \pmod{5}$.

Odgovor: Pravilne so trditve 1,3 in 4.

Kongruence

Lastnosti kongruenc:

1. $a \equiv b \pmod{m}$ natanko takrat ko a in b imata enak ostanek pri deljenju z m;

Kongruence

Lastnosti kongruenc:

1. $a \equiv b \pmod{m}$ natanko takrat ko a in b imata enak ostanek pri deljenju z m;
2. $a \equiv 0 \pmod{m}$ natanko takrat ko je a deljivo z m;

Kongruence

Lastnosti kongruenc:

1. $a \equiv b \pmod{m}$ natanko takrat ko a in b imata enak ostanek pri deljenju z m;
2. $a \equiv 0 \pmod{m}$ natanko takrat ko je a deljivo z m;
3. Naj bo $a \equiv b \pmod{m}$ in $c \equiv d \pmod{m}$. Potem velja

$$a + c \equiv b + d \pmod{m}$$

in

$$ac \equiv bd \pmod{m};$$

Kongruence

Lastnosti kongruenc:

1. $a \equiv b \pmod{m}$ natanko takrat ko a in b imata enak ostanek pri deljenju z m;
2. $a \equiv 0 \pmod{m}$ natanko takrat ko je a deljivo z m;
3. Naj bo $a \equiv b \pmod{m}$ in $c \equiv d \pmod{m}$. Potem velja

$$a + c \equiv b + d \pmod{m}$$

in

$$ac \equiv bd \pmod{m};$$

4. Če je $a \equiv b \pmod{m}$ potem je $a^k \equiv b^k \pmod{m}$, za vsako naravno število k.

Kongruence

Postopek šifriranja zdaj lahko opišemo na naslednji način.
Vsaki črki abecede pridružimo števila (A=0, B=1, . . . , Ž=24).

Postopek šifriranja zdaj lahko opišemo na naslednji način.
Vsaki črki abecede pridružimo števila (A=0, B=1, ..., Ž=24).
Potem pa postopek šifriranja z vporabo Cezarjeve šifre s ključem n lahko definiramo kot funkcijo

$$e : \{0, 1, \ldots, 24\} \to \{0, 1, \ldots, 24\}$$

$$e(x) = x + n \pmod{25}.$$

Kongruence

Postopek šifriranja zdaj lahko opišemo na naslednji način.
Vsaki črki abecede pridružimo števila (A=0, B=1, ..., Ž=24).
Potem pa postopek šifriranja z vporabo Cezarjeve šifre s ključem n lahko definiramo kot funkcijo

$$e : \{0, 1, \ldots, 24\} \to \{0, 1, \ldots, 24\}$$

$$e(x) = x + n \pmod{25}.$$

Postopek dešifriranja pa lahko opišemo z funkcijo

$$d : \{0, 1, \ldots, 24\} \to \{0, 1, \ldots, 24\}$$

$$d(x) = x - n \pmod{25}.$$

Cezarjeva šifra

Koliko varna je Cezarjeva šifra?

Cezarjeva šifra

Koliko varna je Cezarjeva šifra?
Koliko različnih ključev lahko imamo v postopku šifriranja s pomočjo Cezarjeve šifre?

Cezarjeva šifra

Koliko varna je Cezarjeva šifra?
Koliko različnih ključev lahko imamo v postopku šifriranja s pomočjo Cezarjeve šifre?
Odgovor: 25.

Cezarjeva šifra

Koliko varna je Cezarjeva šifra?
Koliko različnih ključev lahko imamo v postopku šifriranja s pomočjo Cezarjeve šifre?
Odgovor: 25.
S pomočjo računalnika bi lahko preverili vseh 25 možnih ključev v zelo kratkem času.

Afina šifra

Spomnimo se da smo v primeru Cezarjeve šifre, potopek šifriranja opisali s pomočjo funkcije. V primeru afine šifre bomo naredili podobno.

Afina šifra

Spomnimo se da smo v primeru Cezarjeve šifre, potopek šifriranja opisali s pomočjo funkcije. V primeru afine šifre bomo naredili podobno.
Vsaki črki abecede pridružimo števila (A=0, B=1, . . . , Ž=24), potem pa postopek šifriranja z vporabo afine šifre lahko definiramo kot funkcijo (v tem primeru vporabimo funkcijo ki se imenuje afina funkcija), oz.

$$e : \{0, 1, \ldots, 24\} \to \{0, 1, \ldots, 24\}$$

$$e(x) = ax + b \pmod{25} \quad \text{za } a, b \in \{0, 1, \ldots, 24\}.$$

Afina šifra

Spomnimo se da smo v primeru Cezarjeve šifre, potopek šifriranja opisali s pomočjo funkcije. V primeru afine šifre bomo naredili podobno.
Vsaki črki abecede pridružimo števila (A=0, B=1, . . . , Ž=24), potem pa postopek šifriranja z vporabo afine šifre lahko definiramo kot funkcijo (v tem primeru vporabimo funkcijo ki se imenuje afina funkcija), oz.

$$e : \{0, 1, \ldots, 24\} \to \{0, 1, \ldots, 24\}$$

$$e(x) = ax + b \pmod{25} \quad \text{za } a, b \in \{0, 1, \ldots, 24\}.$$

V tem primeru ključ je urejen par (a, b).

Afina šifra

Spomnimo se da smo v primeru Cezarjeve šifre, potopek šifriranja opisali s pomočjo funkcije. V primeru afine šifre bomo naredili podobno.
Vsaki črki abecede pridružimo števila (A=0, B=1, . . . , Ž=24), potem pa postopek šifriranja z vporabo afine šifre lahko definiramo kot funkcijo (v tem primeru vporabimo funkcijo ki se imenuje afina funkcija), oz.

$$e : \{0, 1, \ldots, 24\} \to \{0, 1, \ldots, 24\}$$

$$e(x) = ax + b \pmod{25} \quad \text{za } a, b \in \{0, 1, \ldots, 24\}.$$

V tem primeru ključ je urejen par (a, b).
Kaj bi se zgodilo če funkcija e ni injektivna?

Afina šifra

Spomnimo se da smo v primeru Cezarjeve šifre, potopek šifriranja opisali s pomočjo funkcije. V primeru afine šifre bomo naredili podobno.
Vsaki črki abecede pridružimo števila (A=0, B=1, . . . , Ž=24), potem pa postopek šifriranja z vporabo afine šifre lahko definiramo kot funkcijo (v tem primeru vporabimo funkcijo ki se imenuje afina funkcija), oz.

$$e : \{0, 1, \ldots, 24\} \to \{0, 1, \ldots, 24\}$$

$$e(x) = ax + b \pmod{25} \quad \text{za } a, b \in \{0, 1, \ldots, 24\}.$$

V tem primeru ključ je urejen par (a, b).
Kaj bi se zgodilo če funkcija e ni injektivna?
Odgovor: Postopek dešifriranja ne bi bil mogoč.

Afina šifra

Iskaže se da je funkcija $e(x) = ax + b \pmod{25}$ injektivna, če in samo če je $D(a, 25) = 1$ (oziroma če sta števili a in 25 tuji).

Afina šifra

Iskaže se da je funkcija $e(x) = ax + b \pmod{25}$ injektivna, če in samo če je $D(a, 25) = 1$ (oziroma če sta števili a in 25 tuji).
V primeru ko je $a = 1$ dobimo Cezarjevo šifro, torej afina šifra je posplošitev Cezarjeve šifre.

Afina šifra

Iskaže se da je funkcija $e(x) = ax + b \pmod{25}$ injektivna, če in samo če je $D(a, 25) = 1$ (oziroma če sta števili a in 25 tuji).
V primeru ko je $a = 1$ dobimo Cezarjevo šifro, torej afina šifra je posplošitev Cezarjeve šifre.
Za Cezarjevo šifro in afino šifro pravimo, da sta monoabecedni, ker določeno črko vedno zamenjamo z eno isto črko (ki je ponavadi različna od originalne črke).

Afina šifra

Iskaže se da je funkcija $e(x) = ax + b \pmod{25}$ injektivna, če in samo če je $D(a, 25) = 1$ (oziroma če sta števili a in 25 tuji).
V primeru ko je $a = 1$ dobimo Cezarjevo šifro, torej afina šifra je posplošitev Cezarjeve šifre.
Za Cezarjevo šifro in afino šifro pravimo, da sta monoabecedni, ker določeno črko vedno zamenjamo z eno isto črko (ki je ponavadi različna od originalne črke).
Kaj je formula za dešifriranje afine šifre?

Afina šifra

Iskaže se da je funkcija $e(x) = ax + b \pmod{25}$ injektivna, če in samo če je $D(a, 25) = 1$ (oziroma če sta števili a in 25 tuji).
V primeru ko je $a = 1$ dobimo Cezarjevo šifro, torej afina šifra je posplošitev Cezarjeve šifre.
Za Cezarjevo šifro in afino šifro pravimo, da sta monoabecedni, ker določeno črko vedno zamenjamo z eno isto črko (ki je ponavadi različna od originalne črke).
Kaj je formula za dešifriranje afine šifre?
Odgovor:

$$d(x) = c(x - b) \pmod{25},$$

kjer je c tako število za katerega velja $a \cdot c \equiv 1 \pmod{25}$.

Afina šifra

Koliko varna je afina šifra? Koliko različnih ključev imamo v tem primeru?

Afina šifra

Koliko varna je afina šifra? Koliko različnih ključev imamo v tem primeru?
Koliko možnosti imamo za izbiro števila $a \in \{0, 1, \ldots, 24\}$ za katerega velja $D(a, 25) = 1$?

Afina šifra

Koliko varna je afina šifra? Koliko različnih ključev imamo v tem primeru?
Koliko možnosti imamo za izbiro števila $a \in \{0, 1, \ldots, 24\}$ za katerega velja $D(a, 25) = 1$?
Odgovor:
$a \in \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\}$, oz imamo 20 možnosti za a.

Afina šifra

Koliko varna je afina šifra? Koliko različnih ključev imamo v tem primeru?
Koliko možnosti imamo za izbiro števila $a \in \{0, 1, \ldots, 24\}$ za katerega velja $D(a, 25) = 1$?
Odgovor:
$a \in \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\}$,
oz imamo 20 možnosti za a.
Število b je lahko poljubno število iz množice $\{0, 1, 2, \ldots, 24\}$.
Število ključev za afino šifro je $20 \cdot 25$=500.

Afina šifra

Koliko varna je afina šifra? Koliko različnih ključev imamo v tem primeru?
Koliko možnosti imamo za izbiro števila $a \in \{0, 1, \ldots, 24\}$ za katerega velja $D(a, 25) = 1$?
Odgovor:
$a \in \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\}$,
oz imamo 20 možnosti za a.
Število b je lahko poljubno število iz množice $\{0, 1, 2, \ldots, 24\}$.
Število ključev za afino šifro je $20 \cdot 25$=500.
Tudi to število ključev ni veliki problem za računalnik.

Substitucijska šifra

Vsako črko abecede zamenjamo z neko drugo črko, ne glede na to, koliko mest za njo je v abecedi.

Substitucijska šifra

Vsako črko abecede zamenjamo z neko drugo črko, ne glede na to, koliko mest za njo je v abecedi.
Recimo:

A	B	C	Č	...	V	Z	Ž
↓	↓	↓	↓	↓	↓	↓	↓
E	A	M	G	...	B	I	Š

Substitucijska šifra

Koliko različnih možnosti imamo za substitucijsko šifro, oziroma, koliko je pri substitucijski šifri vseh možnih ključev?

Substitucijska šifra

Koliko različnih možnosti imamo za substitucijsko šifro, oziroma, koliko je pri substitucijski šifri vseh možnih ključev?
Odgovor: Vseh možnih ključev je

$$25 \cdot 24 \cdot 23 \ldots 3 \cdot 2 \cdot 1 = 25! = 15511210043330985984000000.$$

Substitucijska šifra

Koliko različnih možnosti imamo za substitucijsko šifro, oziroma, koliko je pri substitucijski šifri vseh možnih ključev?
Odgovor: Vseh možnih ključev je

$$25 \cdot 24 \cdot 23 \ldots 3 \cdot 2 \cdot 1 = 25! = 15511210043330985984000000.$$

Računalnik bi za preverjanje vseh teh možnih ključev rabil približno 500 000 000 let.

Substitucijska šifra

Koliko različnih možnosti imamo za substitucijsko šifro, oziroma, koliko je pri substitucijski šifri vseh možnih ključev?
Odgovor: Vseh možnih ključev je

$$25 \cdot 24 \cdot 23 \ldots 3 \cdot 2 \cdot 1 = 25! = 15511210043330985984000000.$$

Računalnik bi za preverjanje vseh teh možnih ključev rabil približno 500 000 000 let.

Ampak...

Substitucijska šifra

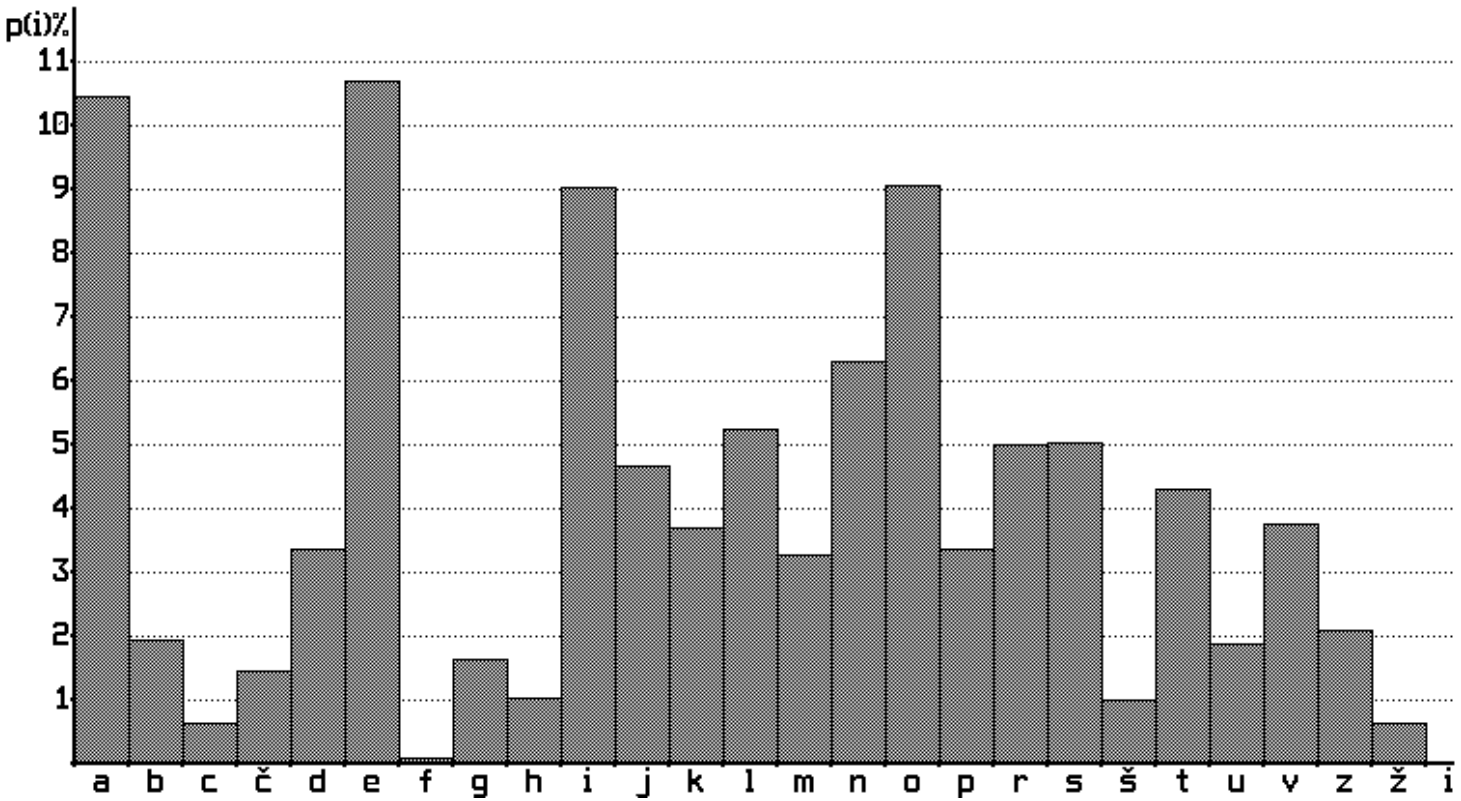
Ali je substitucijska šifra res tako varna?

Substitucijska šifra

Ali je substitucijska šifra res tako varna?
Nekatere črke se pojavljajo bolj pogosto kot preostale.

Substitucijska šifra

Ali je substitucijska šifra res tako varna?
Nekatere črke se pojavljajo bolj pogosto kot preostale.



Slika: Porazdelitev črk v slovenskem jeziku

Substitucijska šifra

Če imamo dovolj dolgo besedilo ki je šifrirano, potem lahko s pomočjo frekvenčne analize razvozlamo substitucijsko šifro.

Vigenerjeva šifra

Slika: Blaise de Vigenère, 1523 – 1596

Vigenerjeva šifra

V Vigenerjevi šifri imamo za ključ besedo dolžine m, kjer je m neko naravno število.

Vigenerjeva šifra

V Vigenerjevi šifri imamo za ključ besedo dolžine m, kjer je m neko naravno število.

Zgled: Zašifriraj besedilo: Sporočilo je skrivnost, z vporabo Vigenerjeve šifre s ključno besedo DAN.

Vigenerjeva šifra

V Vigenerjevi šifri imamo za ključ besedo dolžine m, kjer je m neko naravno število.

Zgled: Zašifriraj besedilo: Sporočilo je skrivnost, z vporabo Vigenerjeve šifre s ključno besedo DAN.

S	P	O	R	O	Č	I	L	O	J	E	S	K	R	I	V	N
D	A	N	D	A	N	D	A	N	D	A	N	D	A	N	D	A
V	P	D	U	O	...											

Vigenerjeva šifra

Vigenerjeva šifra je dosti časa veljala za nezlomljivo, in dolgo časa so jo imenovali "le chiffre indechiffrable", kar pomeni "nezlomljiva šifra".

Vigenerjeva šifra

Vigenerjeva šifra je dosti časa veljala za nezlomljivo, in dolgo časa so jo imenovali "le chiffre indechiffrable", kar pomeni "nezlomljiva šifra".

Nemški oficir Friedrich Kasiski je leta 1863 opisal, kako lahko zlomimo Vigenerjevo šifro. Kasneje so se razvile še druge metode za dešifriranje Vigenerjeve šifre.

Enigma

Slika: Nemška šifrirna naprava ENIGMA v drugi svetovni vojni

Enigma

Enígma je električna naprava za šifriranje sporočil. Uporabljale so jo nemške oborožene sile med 2. svetovno vojno.

Enigma

Enígma je električna naprava za šifriranje sporočil. Uporabljale so jo nemške oborožene sile med 2. svetovno vojno.
Uporabniki ENIGME so bili prepričani, da se njihovo strojno izdelano šifriranje besedil ne da zlomiti z ročnimi metodami, kar je bilo možno za praktično vse sisteme šifriranja do leta 1918. Kar so spregledali, je bilo, da se strojno šifriranje da zlomiti s strojnimi metodami.

Poljska bomba

Skupina poljskih matematikov, zbranih okrog Mariana Rejewskega, je že pred drugo svetovno vojno dosegla velike uspehe pri dešifriranju besedil, šifriranih na ENIGMI.

Poljska bomba

Skupina poljskih matematikov, zbranih okrog Mariana Rejewskega, je že pred drugo svetovno vojno dosegla velike uspehe pri dešifriranju besedil, šifriranih na ENIGMI.
S pomočjo elektromehanskih naprav, tako imenovanih "bomb", je bilo možno v nekaj urah odkriti dnevni ključ, ki se je uporabljal za nastavitve kolutov in so ga Nemci menjali vsak dan točno ob polnoči.

Poljska bomba

Skupina poljskih matematikov, zbranih okrog Mariana Rejewskega, je že pred drugo svetovno vojno dosegla velike uspehe pri dešifriranju besedil, šifriranih na ENIGMI.
S pomočjo elektromehanskih naprav, tako imenovanih "bomb", je bilo možno v nekaj urah odkriti dnevni ključ, ki se je uporabljal za nastavitve kolutov in so ga Nemci menjali vsak dan točno ob polnoči.
Leta 1939 so Nemci izboljšali sestavo ENIGME, tako da so namesto treh uporabljali pet šifrirnih kolutov, od katerih so bili istočasno v uporabi vedno le trije.

Alan Turing

Dva tedna pred nemškim napadom na Poljsko leta 1939 so Poljaki seznanili zaprepadene Angleže in Francoze, ki se jim o ENIGMI še sanjalo ni, o kriptografskih slabostih ENIGME, načrt "bomb" in jim izročili dve na Poljskem izdelani kopiji ENIGME v Veliko Britanijo in Francijo.

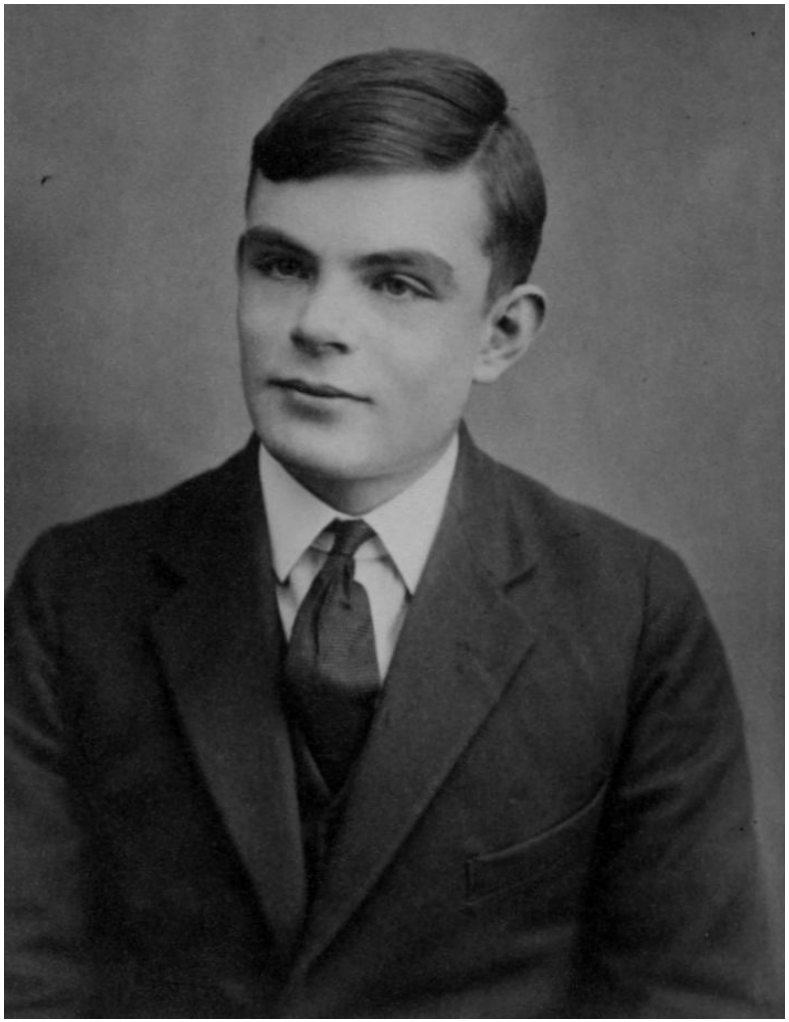
Alan Turing

Dva tedna pred nemškim napadom na Poljsko leta 1939 so Poljaki seznanili zaprepadene Angleže in Francoze, ki se jim o ENIGMI še sanjalo ni, o kriptografskih slabostih ENIGME, načrt "bomb" in jim izročili dve na Poljskem izdelani kopiji ENIGME v Veliko Britanijo in Francijo.
Britanski kriptoanalitiki so delali v Bletchley Parku.

Alan Turing

Dva tedna pred nemškim napadom na Poljsko leta 1939 so Poljaki seznanili zaprepadene Angleže in Francoze, ki se jim o ENIGMI še sanjalo ni, o kriptografskih slabostih ENIGME, načrt "bomb" in jim izročili dve na Poljskem izdelani kopiji ENIGME v Veliko Britanijo in Francijo.
Britanski kriptoanalitiki so delali v Bletchley Parku.
Eden izmed številnih znanstvenikov v Bletchley Parku je bil angleški matematik Alan Turing, eden največjih umov 20. stoletja, katerega dela o računalništvu, matematiki in informatiki so še danes pomembna.

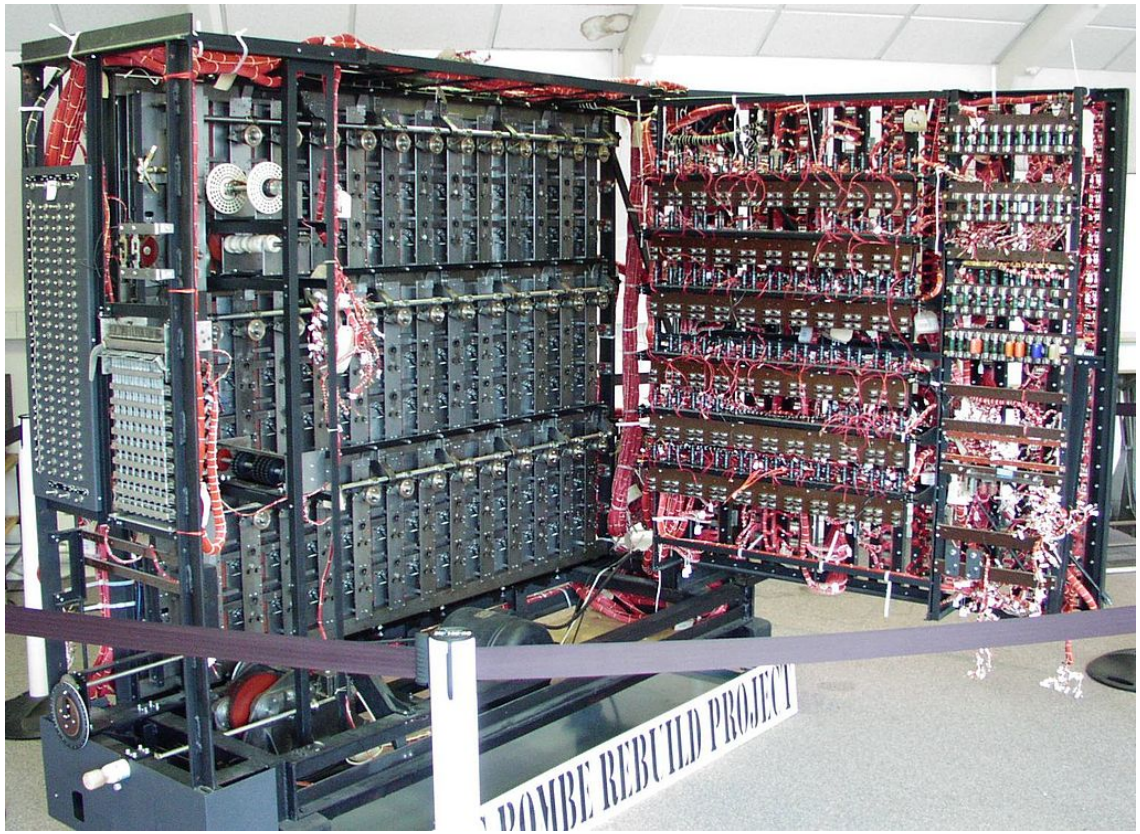
Alan Turing



Slika: Alan Turing, 1912 - 1954

Angleška bomba

Turing je izdelal pomembne osnove za izdelavo angleške, močno izboljšane različice poljske bombe.



Slika: Replika angleške bobme

Angleška bomba

Pri koncu vojne je zaveznikom uspelo dešifrirati večino nemških radijskih sporočil.

Angleška bomba

Pri koncu vojne je zaveznikom uspelo dešifrirati večino nemških radijskih sporočil.

Zgodovinarji domnevajo, da je to razbitje šifer skrajšalo vojno za nekaj mesecev, če ne za celo leto (nekateri trdijo tudi za 2 leti).

Kriptografija javnega ključa

V modelih šifriranja ki smo jih do sedaj predstavili imamo en ključ ki ga vporabljamo za šifriranje in dešifriranje. Problem je z izmenjavo ključa. Da bi z neko odaljeno osebo izmenjavali zaupne informacije, bi si morali prej izmenjati ključ prek varnega kanala.

Kriptografija javnega ključa

V modelih šifriranja ki smo jih do sedaj predstavili imamo en ključ ki ga vporabljamo za šifriranje in dešifriranje. Problem je z izmenjavo ključa. Da bi z neko odaljeno osebo izmenjavali zaupne informacije, bi si morali prej izmenjati ključ prek varnega kanala. Pri kriptografiji javnega ključa, gre za to, da imamo dva različna ključa, javni ključ, s pomočja katerega se sporočila šifrirajo, in zasebni ključ, s pomočjo katerega se sporočila dešifrirajo.

RSA kriptosistem

RSA kriptosistem je primer kriptografije javnega ključa ki so ga leta 1977 razvili Rivest, Shamir in Adleman.
Da bi razumeli postopek šifriranja moramo najprej spoznati Eulerjevo φ funkcija ter Eulerjev izrek.

Eulerjeva funkcija

Za pozitivno naravno število n označino z $\varphi(n)$ število vseh pozitivnih naravnih števil ki ne presegajo n in so tuja z n. Funkcija $\varphi(n)$ se imenuje Eulerjeva funkcija.

Eulerjeva funkcija

Za pozitivno naravno število n označino z $\varphi(n)$ število vseh pozitivnih naravnih števil ki ne presegajo n in so tuja z n. Funkcija $\varphi(n)$ se imenuje Eulerjeva funkcija.
Zgled: $n = 6$, pozitivna naravna števila ki ne presegajo 6 in so tuja s 6 so 1 in 5. Torej $\varphi(6) = 2$.

Eulerjeva funkcija

Za pozitivno naravno število n označino z $\varphi(n)$ število vseh pozitivnih naravnih števil ki ne presegajo n in so tuja z n. Funkcija $\varphi(n)$ se imenuje Eulerjeva funkcija.
Zgled: $n = 6$, pozitivna naravna števila ki ne presegajo 6 in so tuja s 6 so 1 in 5. Torej $\varphi(6) = 2$.
Lastnosti Eulerjeve funkcije:

1. Če je p praštevilo, potem je $\varphi(p) = p - 1$;
2. Če sta m in n tuji si števili, potem je $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

Eulerjev izrek

Theorem

Če je n pozitivno naravno število, in je x število ki je tuje z n potem je $x^{\varphi(n)} \equiv 1 \pmod{n}$.

Eulerjev izrek

Theorem

Če je n pozitivno naravno število, in je x število ki je tuje z n potem je $x^{\varphi(n)} \equiv 1 \pmod{n}$.

Posledica Eulerjevega izreka:

$$x^{k\cdot\varphi(n)} \equiv 1 \pmod{n}$$

Eulerjev izrek

Theorem

Če je n pozitivno naravno število, in je x število ki je tuje z n potem je $x^{\varphi(n)} \equiv 1 \pmod{n}$.

Posledica Eulerjevega izreka:

$$x^{k\cdot\varphi(n)} \equiv 1 \pmod{n}$$

$$x^{k\cdot\varphi(n)+1} \equiv x \pmod{n}$$

Eulerjev izrek

Theorem

Če je n pozitivno naravno število, in je x število ki je tuje z n potem je $x^{\varphi(n)} \equiv 1 \pmod{n}$.

Posledica Eulerjevega izreka:

$$x^{k\cdot\varphi(n)} \equiv 1 \pmod{n}$$

$$x^{k\cdot\varphi(n)+1} \equiv x \pmod{n}$$

V RSA kriptosistemu bomo imeli par števil d in e, tako da je $d \cdot e = k \cdot \varphi(n) + 1$.

1. Izberejo se dve različni praštevili p in q;

1. Izberejo se dve različni praštevili p in q;
2. Izračuna se $n = p \cdot q$; (n je vsem dostopen in se vporablja kot modul za javni in zasebni ključ);

1. Izberejo se dve različni praštevili p in q;
2. Izračuna se $n = p \cdot q$; (n je vsem dostopen in se vporablja kot modul za javni in zasebni ključ);
3. Izračuna se $\varphi(n) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1)$;

1. Izberejo se dve različni praštevili p in q;
2. Izračuna se $n = p \cdot q$; (n je vsem dostopen in se vporablja kot modul za javni in zasebni ključ);
3. Izračuna se $\varphi(n) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1)$;
4. Izbere se naravno število e, tako da je $1 < e < \varphi(n)$ tako da sta si e in $\varphi(n)$ tuji (e je vsem dostopen, in se vporablja kot eksponent javnega ključa);

1. Izberejo se dve različni praštevili p in q;
2. Izračuna se $n = p \cdot q$; (n je vsem dostopen in se vporablja kot modul za javni in zasebni ključ);
3. Izračuna se $\varphi(n) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1)$;
4. Izbere se naravno število e, tako da je $1 < e < \varphi(n)$ tako da sta si e in $\varphi(n)$ tuji (e je vsem dostopen, in se vporablja kot eksponent javnega ključa);
5. Izračuna se d, tako da je $e \cdot d \equiv 1 \pmod{\varphi(n)}$ (d je zasebni ključ).

1. Izberejo se dve različni praštevili p in q;
2. Izračuna se $n = p \cdot q$; (n je vsem dostopen in se vporablja kot modul za javni in zasebni ključ);
3. Izračuna se $\varphi(n) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1)$;
4. Izbere se naravno število e, tako da je $1 < e < \varphi(n)$ tako da sta si e in $\varphi(n)$ tuji (e je vsem dostopen, in se vporablja kot eksponent javnega ključa);
5. Izračuna se d, tako da je $e \cdot d \equiv 1 \pmod{\varphi(n)}$ (d je zasebni ključ).

Javni ključ: (n, e).
Zasebni ključ: d. (Vrednosti p in q tudi morajo biti skrite, ker se s pomočjo njih lahko izračuna vrednost d).

Postopek šifriranja:

1. A: pošlje javni ključ (n, e) osebi B in hrani d kot zasebni ključ.

Postopek šifriranja:

1. A: pošlje javni ključ (n, e) osebi B in hrani d kot zasebni ključ.
2. B: želi poslati sporočilo M. Najprej svoje sporočilo zapiše v obliki števila m, tako da je $0 \leq m < n$.

Postopek šifriranja:

1. A: pošlje javni ključ (n, e) osebi B in hrani d kot zasebni ključ.
2. B: želi poslati sporočilo M. Najprej svoje sporočilo zapiše v obliki števila m, tako da je $0 \leq m < n$.
3. B: izračuna vrednost $c \equiv m^e \pmod{n}$. c je šifrirano sporočilo ki ga B pošlje osebi A;

Postopek šifriranja:

1. A: pošlje javni ključ (n, e) osebi B in hrani d kot zasebni ključ.
2. B: želi poslati sporočilo M. Najprej svoje sporočilo zapiše v obliki števila m, tako da je $0 \leq m < n$.
3. B: izračuna vrednost $c \equiv m^e \pmod{n}$. c je šifrirano sporočilo ki ga B pošlje osebi A;

Postopek dešifriranja:

1. A s pomočjo tajnega ključa d računa vrednost $m \equiv c^d \pmod{n}$.

Postopek šifriranja:

1. A: pošlje javni ključ (n, e) osebi B in hrani d kot zasebni ključ.
2. B: želi poslati sporočilo M. Najprej svoje sporočilo zapiše v obliki števila m, tako da je $0 \leq m < n$.
3. B: izračuna vrednost $c \equiv m^e \pmod{n}$. c je šifrirano sporočilo ki ga B pošlje osebi A;

Postopek dešifriranja:

1. A s pomočjo tajnega ključa d računa vrednost $m \equiv c^d \pmod{n}$.
2. Iz števila m se potem pride do začetnega sporočila M.

Postopek šifriranja:

1. A: pošlje javni ključ (n, e) osebi B in hrani d kot zasebni ključ.
2. B: želi poslati sporočilo M. Najprej svoje sporočilo zapiše v obliki števila m, tako da je $0 \leq m < n$.
3. B: izračuna vrednost $c \equiv m^e \pmod{n}$. c je šifrirano sporočilo ki ga B pošlje osebi A;

Postopek dešifriranja:

1. A s pomočjo tajnega ključa d računa vrednost $m \equiv c^d \pmod{n}$.
2. Iz števila m se potem pride do začetnega sporočila M.

Dokaz pravilnosti: Ker je $ed = 1 + k \cdot \varphi(n)$ potem je c^d

Postopek šifriranja:

1. A: pošlje javni ključ (n, e) osebi B in hrani d kot zasebni ključ.
2. B: želi poslati sporočilo M. Najprej svoje sporočilo zapiše v obliki števila m, tako da je $0 \leq m < n$.
3. B: izračuna vrednost $c \equiv m^e \pmod{n}$. c je šifrirano sporočilo ki ga B pošlje osebi A;

Postopek dešifriranja:

1. A s pomočjo tajnega ključa d računa vrednost $m \equiv c^d \pmod{n}$.
2. Iz števila m se potem pride do začetnega sporočila M.

Dokaz pravilnosti: Ker je $ed = 1 + k \cdot \varphi(n)$ potem je $c^d \equiv (m^e)^d \equiv m^{ed} \equiv m \pmod{n}$.

RSA-zgled

Recimo da so izbrane vrednosti $p = 7$ in $q = 17$. Potem je $n = 7 \cdot 17 = 119$ in $\varphi(n) = 6 \cdot 16 = 96$. Število e je lahko poljubno število od 2 do 95 tako da je e tuje s 96.

RSA-zgled

Recimo da so izbrane vrednosti $p = 7$ in $q = 17$. Potem je $n = 7 \cdot 17 = 119$ in $\varphi(n) = 6 \cdot 16 = 96$. Število e je lahko poljubno število od 2 do 95 tako da je e tuje s 96.
Recimo da se izbere vrednost $e = 5$.

RSA-zgled

Recimo da so izbrane vrednosti $p = 7$ in $q = 17$. Potem je $n = 7 \cdot 17 = 119$ in $\varphi(n) = 6 \cdot 16 = 96$. Število e je lahko poljubno število od 2 do 95 tako da je e tuje s 96.
Recimo da se izbere vrednost $e = 5$. Zdaj je treba izračunati vrednost d tako da je $d \cdot e \equiv 1 \pmod{96}$. Kako učinkovito izračunati vrednost d? Lahko vporabimo Euklidov algoritem:

$$96 = 5 \cdot 19 + 1$$

Torej $1 = 1 \cdot 96 - 5 \cdot 19$, oz. $d \equiv -19 \equiv 77 \pmod{96}$.

RSA-zgled

Javni ključ: $n = 119, e = 5$.
Zasebni ključ: $d = 77$.

RSA-zgled

Javni ključ: $n = 119, e = 5$.
Zasebni ključ: $d = 77$.
Recimo da je sporočilo ki ga želimo poslati črka F. Potem besedilo zapišemo kot številko, recimo $m = 6$.

RSA-zgled

Javni ključ: $n = 119, e = 5$.
Zasebni ključ: $d = 77$.
Recimo da je sporočilo ki ga želimo poslati črka F. Potem besedilo zapišemo kot številko, recimo $m = 6$.
$c = m^e = 6^5 \equiv 41 \pmod{119}$.

RSA-zgled

Javni ključ: $n = 119, e = 5$.
Zasebni ključ: $d = 77$.
Recimo da je sporočilo ki ga želimo poslati črka F. Potem besedilo zapišemo kot številko, recimo $m = 6$.
$c = m^e = 6^5 \equiv 41 \pmod{119}$.
Šifrirano sporočilo je 41.
Za dešifriranje se izračuna vrednost $c^d = 41^{77} \equiv 6 \pmod{119}$.

Varnost RSA

Varnost RSA kriptosistema slovi na težavnosti faktorizacije naravnih števil na produkt praštevil. Posebej težavna za faktorizacijo (z vporabo do sedaj znanih algoritmov) so polpraštevila, oz. števila ki so produkt dveh praštevil. Ko sta obe praštevili veliki naključno izbrani različni praštevili približno enake velikosti, potem tudi z vporabo najbolj močnih računalnikov je potrebno preveč časa da bi se naredila faktorizacija (z vporabo do sedaj znanih algoritmov).

Varnost RSA

Varnost RSA kriptosistema slovi na težavnosti faktorizacije naravnih števil na produkt praštevil. Posebej težavna za faktorizacijo (z vporabo do sedaj znanih algoritmov) so polpraštevila, oz. števila ki so produkt dveh praštevil. Ko sta obe praštevili veliki naključno izbrani različni praštevili približno enake velikosti, potem tudi z vporabo najbolj močnih računalnikov je potrebno preveč časa da bi se naredila faktorizacija (z vporabo do sedaj znanih algoritmov). Leta 1991 je objavljen "RSA factoring challenge" za faktorizacijo danih polpraštevil. Večina zastavljenih števil še vedno ni faktorizirana. Na primer, leta 2009 je skupina raziskovalcev uspešno faktorizirala 232-mestno število z vporabo več sto močnih računalnikov ki so delali več kot dve leti. Čas računanja na enem navadnem računalniku bi bil približno 2000 let.

Hvala za pozornost!!!