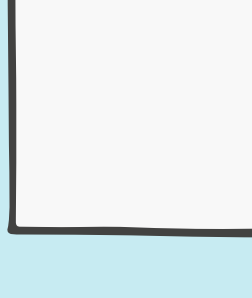
Kriptografija

- veda o varnem komuniciranju
- ukvarja se z naslednjimi vprašanji:
  - Kako poskrbeti za varnost na internetu?
  - Kako shranjevati gesla, da jih nepridipravi ne morejo izvedeti?
  - Kako preverjati, da sporočil, ki jih pošiljamo po internetu, kdo ne prestreže in spremeni ter podobno?
- pogosto se zgodi, da moramo sporočiti nekomu podatke, ki jih ne želimo razkriti
- šifra je besedilo, napisano v skrivnih znakih
  - Zakaj?
    - To storimo zato, da ga razume samo oseba, ki ga zna dešifrirati.
- dešifrirati pomeni, da oseba iz skrivnih zapisov spremeni nazaj v smiselno besedo



Cezarjeva šifra

- Je eden od primerov enostavnega šifriranja.
- Gre za zamenjavo, kjer se vsaka črka zamenja z drugo črko v abecedi, zamaknjeno za določeno število mest
- **način šifriranja**: vse A-je zamenjamo z B-ji, vse B-je zamenjamo s C-ji, vse C-je s Č-ji in tako naprej. Na koncu Ž zamenjamo z A-ji.
  - spodaj je prikaza tabela za pomoč

A	B	C	Č	D	E	F	G	I	J	K	L	M
B	C	Č	D	E	F	G	I	J	K	L	M	N

premik enega znaka abecede v levo

N	O	P	R	S	Š	T	U	V	Z	Ž
O	P	R	S	Š	T	U	V	Z	Ž	A

- šifriranje -premik v levo
  - geslo: ŽAN ŠIFRIRA
  - šifra: ABO TJGSJSB
- dešifriranje - premik v desno
  - širfa: NJB CDPD
  - geslo: MIA BERE