- One Time Pad
- Opis
- Nedostaci
- Primena
- Rezime

Kriptologija 1

One Time Pad

- One Time Pad
- Opis
- Nedostaci
- Primena
- Rezime

- Šifrovanje jednokratnim ključem (eng. one-time pad - OTP)
- Ova metoda je u upotrebi od 1917.
- Otvoreni tekst se kombinuje sa slučajnim ključem koji je podjednako dug kao i tekst koji se šifruje.
- Ključ se u komunikaciji koristi samo jedanput i nikada više
- Spaja se sa otvorenim tekstom koristeći XOR.
- Treba da postoje 2 kopije ključa.

Opis

- One Time Pad
- Opis
- Nedostaci
- Primena
- Rezime

- Svi podaci se predstavljaju u binarnom obliku. Šifrat se iz otvorenog teksta dobija primenom operacije „ekskluzivno ili“ (XOR) za otvoreni tekst i ključ.
  - $C = P \oplus K$
- Postupak dešifrovanja je identičan postupku šifrovanja:
  - $P = C \oplus K$

Šifrovanje

- One Time Pad
- Opis
- Nedostaci
- Primena
- Rezime

PORUKA	S	I	N	G	I	D	U	N	U	M
M	000	001	010	011	001	100	101	010	101	110
K	010	010	110	110	100	010	101	011	110	010
C	010	011	100	101	101	110	000	001	011	100
ŠIFRAT	N	G	D	U	U	M	S	I	G	D

Dešifrovanje

- One Time Pad
- Opis
- Nedostaci
- Primena
- Rezime

ŠIFRAT	N	G	D	U	U	M	S	I	G	D
C	010	011	100	101	101	110	000	001	011	100
K	010	010	110	110	100	010	101	011	110	010
M	000	001	010	011	001	100	101	010	101	110
PORUKA	S	I	N	G	I	D	U	N	U	M

Dešifrovanje lažnim ključem

- One Time Pad
- Opis
- Nedostaci
- Primena
- Rezime

ŠIFRAT	N	G	D	U	U	M	S	I	G	D
C	010	011	100	101	101	110	000	001	011	100
K	001	010	110	100	101	011	010	000	011	001
M	011	001	010	001	000	101	010	001	000	101
PORUKA	G	I	N	I	S	U	N	I	S	U

Nedostaci

- One Time Pad
- Opis
- Nedostaci
- Primena
- Rezime

- Do sada je dokazano da je šifrovanje jednokratnim ključem od slučajnog niza, koji se koristi samo jedanput i tajan je, kao kriptografska metoda teoretski neslomljivo.

- U slučaju da se koristi dva puta isti ključ kriptoanalitičar lako može da sazna otvoreni tekst druge poslate poruke na osnovu snimljenih šifrata za obe poruke i poznatog otvorenog teksta prve poruke.

Primena

- One Time Pad
- Opis
- Nedostaci
- Primena
- Rezime

- Projekat „VENONA“ predstavlja One Time Pad u realnom životu.
- Sovjetska špijunska mreža formirana je na teritoriji SAD 40-tih godina prošlog veka. U pitanju je bila nuklearna špijunaža.
- Za jednu ovaku akciju je bilo neophodno razmeniti na hiljade šifrovanih poruka.
- Međutim, sovjetski špijuni su uneli ključeve prilikom ulaska u SAD. Šifru su koristili na pravilan način iz sigurnosnih razloga.
- Ponavljanje ključa daje realnu mogućnost za probijanje poruka.

Rezime

- One Time Pad
- Opis
- Nedostaci
- Primena
- Rezime

- Šifrat ne daje nikaku informaciju o otvorenom tekstu.
- Svaki otvoreni tekst iste dužine je podjednako verovatan.
- Ključ mora biti slučajan, mora se koristiti samo jedaput.
- Ključ je poznat samo pošiljaocu i primaocu.
- Ključ je iste dužine kao i poruka.
- Mehanizam integriteta ne postoji.

Univerzitet Singidunum

Hvala na pažnji !