

Sigurnije korištenje šifri

Uputstvo za korištenje KeePass-a

KeePass je program za upravljanje lozinkama (*password manager*) otvorenog koda (*open source*). Danas je uobičajeno koristiti veliki broj lozinki za pristup raznim internet stranicama, društvenim mrežama, e-mail serverima i slično. Loša praksa je koristiti istu lozinku za pristup svim ovim sadržajima jer postoji opasnost, da neko, ukoliko sazna vašu lozinku, može istu iskoristiti i zloupotrebiti.

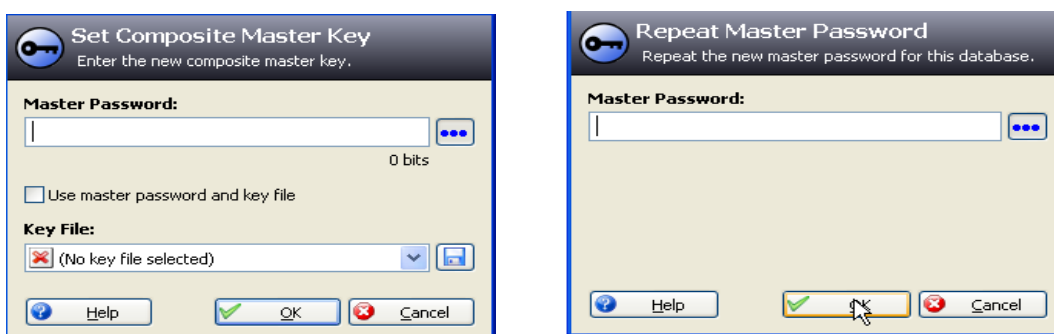
S druge strane, pravljenje više različitih lozinki koje zadovoljavaju standarde sigurnosti (kombinacija malih i velikih slova, brojeva i specijalnih znakova), nameće pitanje pamćenja, odnosno sigurnosti pohranjivanja lozinki na način da budu dostupne samo vama.

Program KeePass, nudi baš ovo. Formira bazu podataka za lozinkama zaštićenu glavnom lozinkom (*Master Password*).

1 Preuzimanje i pokretanje programa

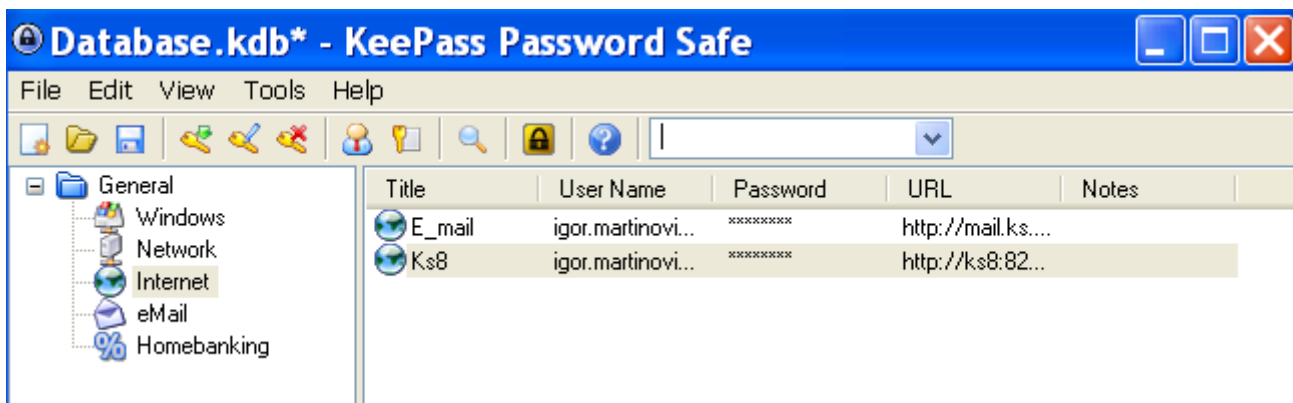
Link za preuzimanje ovog programa je: <http://keepass.info/download.html>. Sa učitane stranice preuzeti prijenosnu verziju [Portable KeePass 1.18 \(ZIP Package\)](#) Nakon preuzimanja dokumenta, raspakovati ga, te pokrenuti.

Nakon pokretanja programa, biće vam zatraženo da ukucate **MasterPassword**te, nakon upisivanja i klika mišem na **OK**, da isti ponovite



Nakon ovoga, dobićete poruku da je **MasterPassword** formiran.

Samo korištenje programa je vrlo jednostavno. Na slici ispod možete vidjeti, u lijevom dijelu prozora, da su već formirane grupe za grupisanje lozinki.



2 Grupe

Novu grupu možete vrlo lako dodati na dva načina. U meniju **Edit** komandom **Add Group** ili istom komandom preko menija koji se otvara pritiskom desne tipke mišem bilo gdje u dijelu prozora sa grupama.

Što se tiče same baze u kojoj će biti sakriveni podaci o lozinkama, ona se automatski formira, ali je moguće formirati novu izborom komande **New** u meniju **File**. Ako ovo uradite, ponovo ćete morati napraviti **Master Password**, na isti način kao i prvi put, ali vjerovatno nećete imati potrebe za više od jedne baze na svom računaru.

3 Dodavanje stranica i lozinki

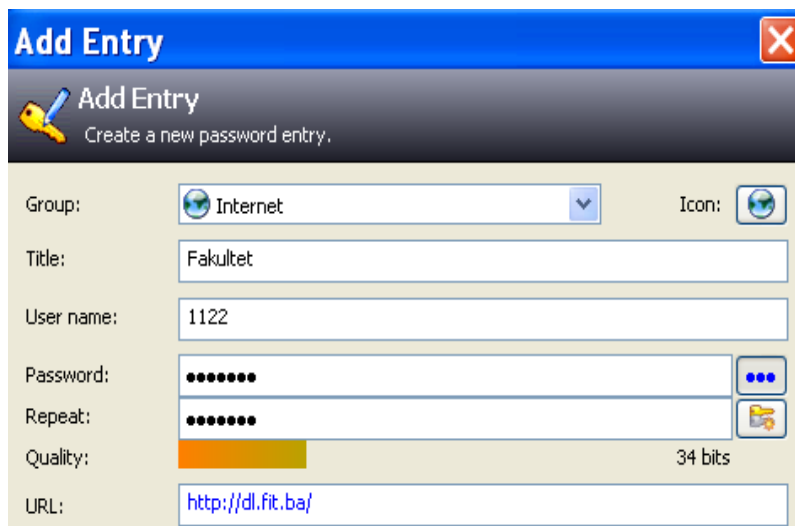
Samo dodavanje podataka u određenu grupu je vrlo jednostavno. Kliknite mišem na naziv grupe, te je na taj način selektujete. U meniju **Edit** izvršite komandu **Add Entry**:



U polju **Group** vidjećete naziv grupe koju ste izabrali.

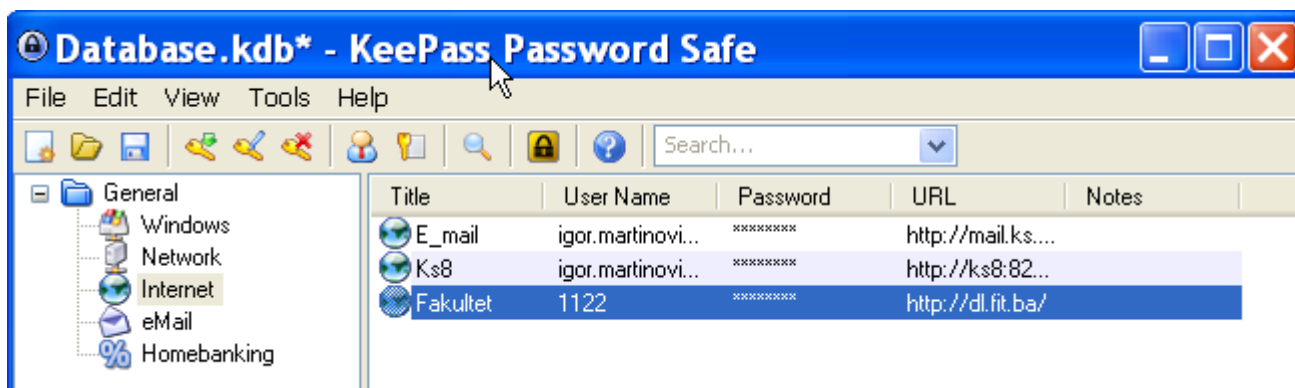
U polje **Title** upišite naziv stranice (ovo nije URL već naziv koji će vas asociirati na stranicu).

U polje **Username** treba upisati korisničko ime, te u polje **Password** lozinku za pristup. I ovdje lozinku treba upisati dva puta zbog smanjenja mogućnosti pojave greške.



Nakon što su polja, kao na slici, popunjena, pritisnuti **OK**.

Ako je sve urađeno kako treba, u desnom dijelu prozora pojaviće se podaci o novounesenom zapisu.

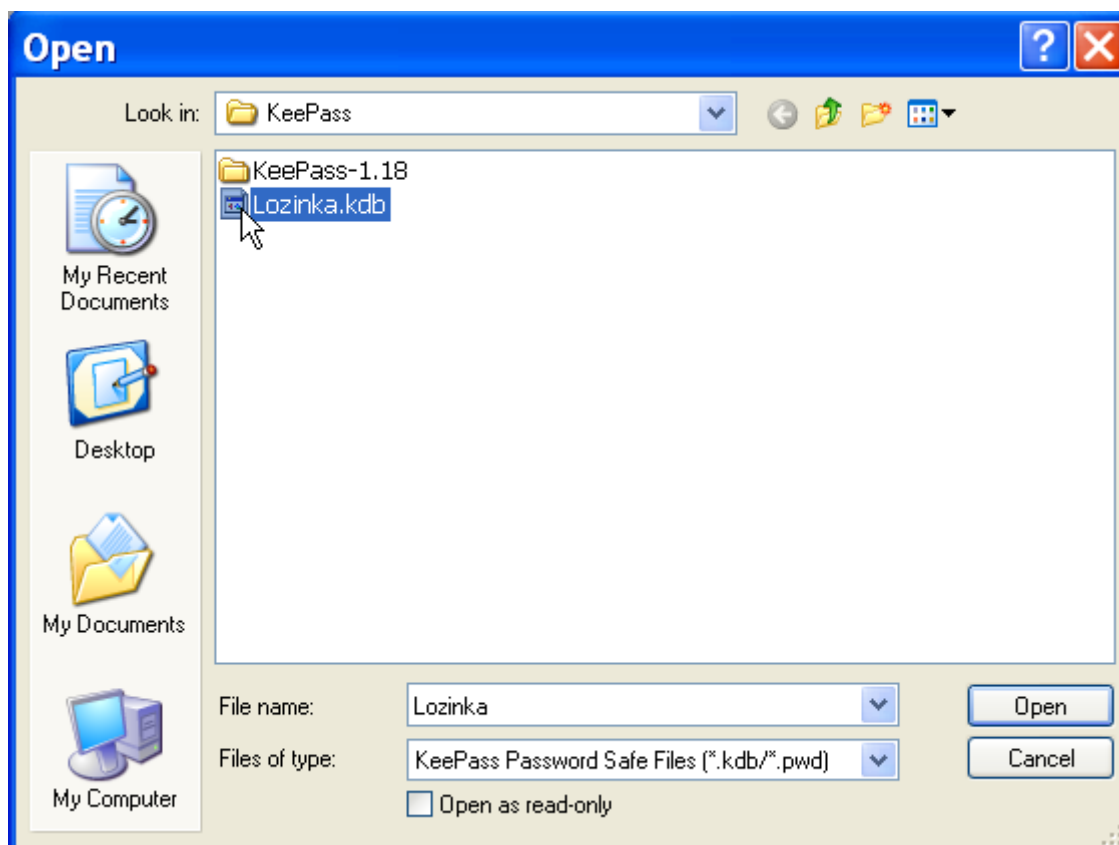


4 Spašavanje baze podataka

Slijedeći korak je spašavanje baze podataka sa lozinkama. Dovoljno je otići u meni **File** i izabrati komandu **Save**. Ova komanda otvara dobro poznati prozor u kome možete izabrati mjesto na disku i naziv baze, te pritiskom na **SAVE** izvršiti spašavanje u formatu .kdb, npr Lozinke.kdb.

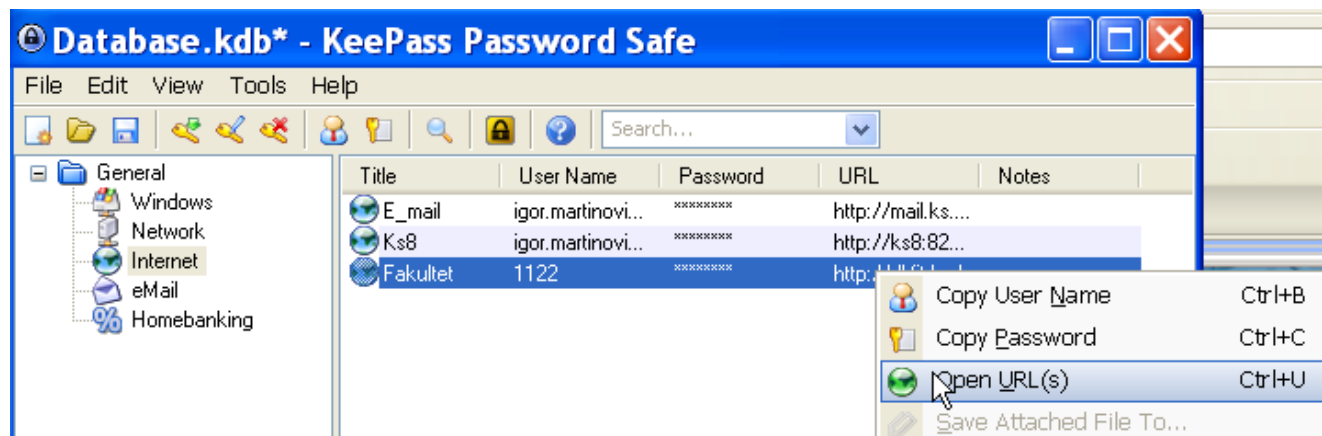
5 Pristup stranicama sa pristupnim podacima

Pokrenite program te u meniju **File** izaberite komandu **Open**:



Nađite sačuvanu bazu te je otvorite. **KeePass** će vam zatražiti upisivanje **Master Password-a**. Nakon upisivanja istog, otvoriće se početni prozor.

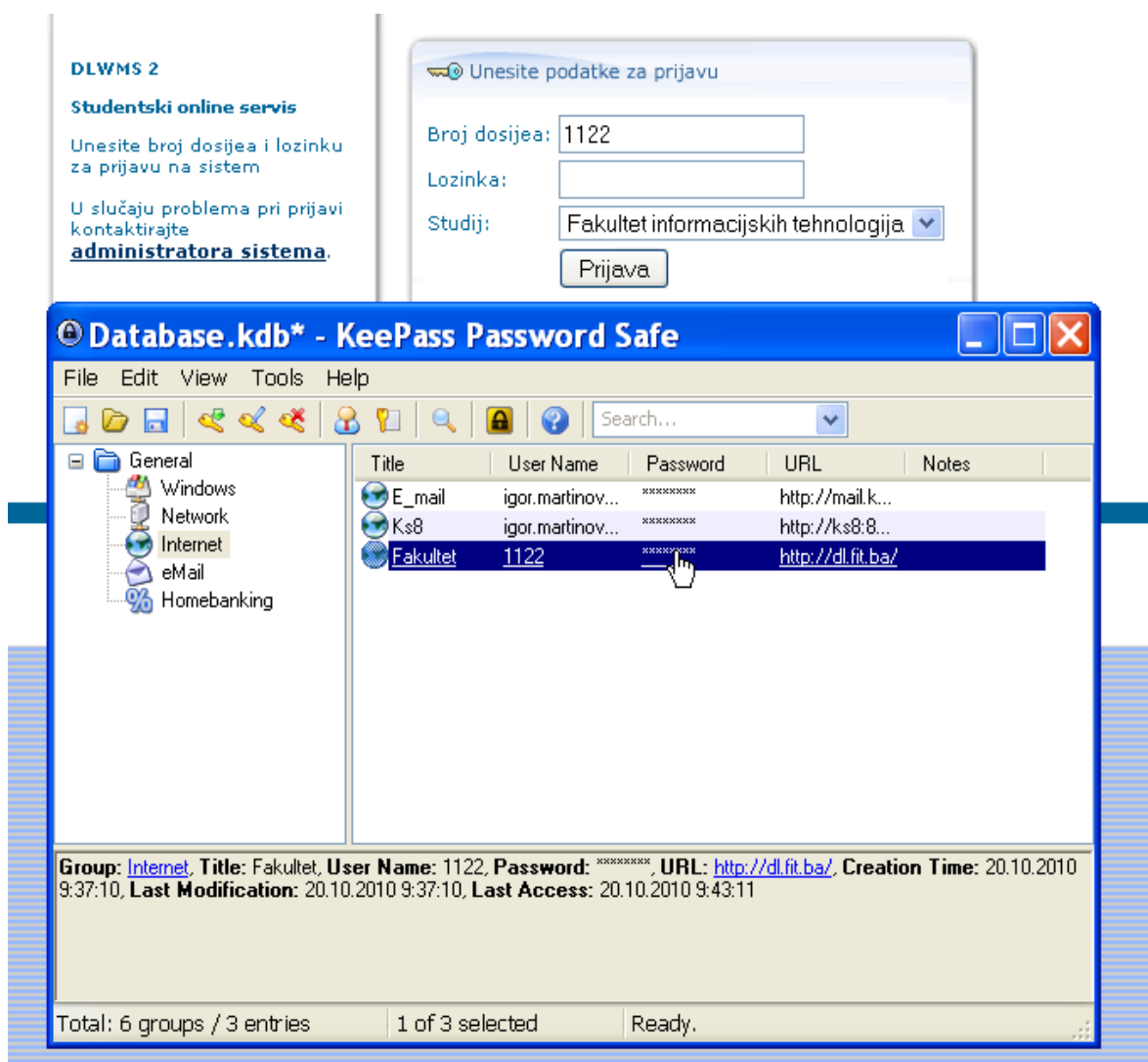
Nakon što se otvori početni prozor, odaberite ciljanu grupu, te u njoj označite stranicu koju želite otvoriti. Dok je miš pozicioniran na željenu stranicu, pritisnite desnu tipku miša i odaberite komandu **Open Url(s)**. Ovu komandu možete naći i u meniju **Edit**.



Direktan pristup na željenu adresu moguć je i sa linka na dnu prozora. Na slici je vidljiv link: **URL: <http://dl.fit.ba>** .



Šta god da odaberete, komanda će izvršiti učitavanje stranice. Na slijedećoj slici vidjećete način pristupa na jednu od izabranih stranica:



U polju **Broj dosjea** upisan je **Username**, a polje **Lozinka** možete popuniti na dva načina. Prvi je da pritisnete mišem na dio sa zvjezdicama koje označavaju **Password** i, ne puštajući tipku miša, povučete **Password** u polje sa lozinkom.

Drugi način je da, na istom mjestu, pritisnete desnu tipku miša da biste dobili pomoćni meni.

Izaberite **Copy Password**, te u polje sa lozinkom izvršite komandu **Paste**. Komandu **Paste** možete izvršiti istovremenim pritiskom tipki **Ctrl** i **V**. Komanda **Copy Password** dostupna je i u meniju **Edit**.

Izvršite prijavljivanje na stranicu.



Na kraju, jedna od boljih stvari kod **KeePass** je to što i program i bazu ne morate imati na disku na računaru. Program se pokreće bez instalacije što znači da i program i bazu možete imati na USB-u, CD-u ili bilo kojem drugom mediju i prenijeti ih na drugi računar.

Jedino ograničenje je u tome ako vam je baza na CD-u moći ćete je otvoriti samo kao **Read Only**, ali će sve funkcije za pristup raditi bez greške.

6 Uputstva za pravilno postupanje sa šiframa

Ova uputstva su objavljena na intranet stranici Kantona, zajedno sa uputstvo za postupanje sa Windows šiframa. Ovdje ih ponavljamo.

* **Mijenjajte** povremeno šifre. **Nemojte** ponovno koristiti stare šifre. **Nemojte** koristiti šifre koje se sastoje od riječi iz rječnika, datuma rođenja, imena porodice, naziva grada, sportskog kluba ili firme, adrese, ili bilo koje druge lične informacije. Ne koristite ponovljene znakove kao što su 111 ili sekvence poput ABC, QWERTY, ili 123 u bilo kojem dijelu vaše od šifre. U suprotnom, šifre se jednostavno mogu predvidjeti ili se brzo razbijaju metodom velikog broja računarski generisanih pokušaja.

* Koristite **program za upravljanje šiframa** (password manager) kako bi čuvali Vaše šifre.

* Držite Vaše šifre **u tajnosti**. Stavljajući ih u datoteku na Vašem računaru, šaljući ih u e-mailu drugima, ili zapisujući ih na komad papira na stolu kao da ste ih dali drugima. Ako morate nekome drugom omogućiti pristup računaru, napravite privremenu šifru samo za njih, a zatim je promijenite odmah nakon toga.

Drugi razlog za korištenje je pamćenje recimo Windows šifre ako koristite enkripciju tj. šifrovanje podataka. Gubitak Windows šifre bi značio i gubitak podataka.

* **Nemojte koristiti istu šifru** za različite web stranice, niti kao Windows ili e-mail šifru. Inače, netko ko uprati Vašu email šifru može otvoriti i Vaš Facebook itd.

* Ako koristite pristup stranicama zaštićenim šifrom preko otvorenih bežičnih mreža - ili bilo koje druge mreže u koju nemate povjerenja - koristite samo **https://** adrese a ne **http://**. Na ovaj način koristite **zaštićeni protokol**. Na donjoj traci sa sličicama u pretraživaču u tom slučaju imate mali katanac.

* Ne unosite šifru ili čak i naziv računa na bilo koju web stranicu kojoj možete pristupiti putem **linka u e-mailu**. To su najvjerojatnije krađe identiteta. Umjesto toga, unesite adresu (URL) direktno u Vaš preglednik, pa otiđite na tu stranicu.