# Enkriptiranje povezav do anket

String s parametri se kriptira z AES256 enkripcijo, na 1KA strani se pa potem dekriptira. Na obeh straneh bi zato imeli nek skriven kljuc za enkripcijo/dekripcijo.

Vzame se samo string s paremetri (ki se je do sedaj poslla preko url v cisti obliki), se ga zakriptira z ustreznim kljucem in potem ta kriptiran string poslje v obliki parametra "params".

Zraven je vključen primer funkcije za enkripcijo v PHP, ki je na strani 1KA stestirana in deluje.

## Anketa PRED izpitom

http://ul.1ka.si/main/survey/evalvacija\_uni.php?params=kriptiraniParametri

Parametri:

* fakulteta=kraticaFakultete
* anketa=idAnkete
* predmet=idPredmeta
* student=md5SifraStudenta

## Anketa PO izpitu

http://ul.1ka.si/main/survey/evalvacija2\_uni.php?params=kriptiraniParametri

Parametri:

* fakulteta=kraticaFakultete
* anketa=idAnkete
* predmet=idPredmeta
* student=md5SifraStudenta

## Splošna anketa

http://ul.1ka.si/main/survey/studentska\_anketa\_uni.php?params=kriptiraniParametri

Parametri:

* fakulteta=kraticaFakultete
* anketa=idAnkete
* student=md5SifraStudenta

## Podiplomska anketa

http://ul.1ka.si/main/survey/podiplomska\_anketa\_uni.php?params=kriptiraniParametri

Parametri:

* fakulteta=kraticaFakultete
* anketa=idAnkete
* student=md5SifraStudenta

## Splošno o parametrih:

* student -> ID študenta zakodiran z md5
* predmet -> ID predmeta ki ga študent rešuje
* fakulteta -> kratica fakultete (fdv, fgg, fri...)
* anketa -> ID ankete (se pošlje ko je anketa izdelana in pripravljena – vsako leto druga)

Vse povezave preusmerijo študenta na ustrezno anketo. Če je študent anketo že izpolnil, se mu prikaže opozorilo: »Anketo za ta predmet ste že izpolnili. Hvala za sodelovanje.«

## Enkripcija parametrov (le za povezave do anket in ne za preverjanje rešene anket):

Zaradi varnosti se pri povezavah na ankete parametri kriptirajo z AES256 (CBC način). To pomeni da je potrebno izvesti enkripcijo vseh parametrov:

* najprej se generira naključen inicializacijski vektor (16 znakov)
* z ustreznim ključem (bo poslan naknadno) in iv se izvede enkripcija AES256 (CBC) na stringu s parametri (npr. *fakulteta=FDV&anketa=123&predmet=1234&student=md5SifraStudenta*)
* kriptiranemu besedilu se na zacetek pripne naključno generiran inicializacijski vektor in izvede base64 encoding:

*base64\_encode($iv.$stringEncrypted);*

Kriptirano besedilo se potem pošlje preko parametra »params«. Primer končne oblike povezave:

http://ul.1ka.si/main/survey/evalvacija2\_uni.php?params=kriptirani\_parametri

**Primer funkcije za enkripcijo v PHP:**

*// Besedilo ki ga kriptiramo*

*$stringClear = 'fakulteta=FDV&anketa=123&predmet=1234&student=md5SifraStudenta'*

*// Kljuc v hex pretvorimo v binary*

*$aes256Key = pack('H\*',"1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef");*

*// Generiramo random iv*

*$iv = mcrypt\_create\_iv(mcrypt\_get\_iv\_size(MCRYPT\_RIJNDAEL\_128, MCRYPT\_MODE\_CBC), MCRYPT\_RAND);*

*// Kriptiramo besedilo z AES256 CBC*

*$stringEncrypted = mcrypt\_encrypt(MCRYPT\_RIJNDAEL\_128, $aes256Key, $stringClear, MCRYPT\_MODE\_CBC, $iv);*

*// Pripnemo iv in encodamo*

*$stringEncrypted = base64\_encode($iv.$stringEncrypted);*

*return $stringEncrypted;*

# Preverjanje rešenosti anket (za prijavo študenta na izpit)

## Preverjanje za anketo PRED izpitom

http://ul.1ka.si/main/survey/studentska\_prijava\_uni.php?fakulteta=kraticaFakultete&student=md5SifraStudenta&predmeti=idPredmeta1xidPredmeta2xidPredmeta3

Skripta vrne string v JSON formatu s polji:

* student
  + ID študenta zakodiran z md5, za katerega se izvaja preverjanje
* prijava
  + false, če se ne dovoli prijave, ker niso rešene ankete za vse predmete
  + true, če se dovoli prijava, ker so ankete za vse predmete rešene
* predmeti\_nereseni
  + ID-ji predmetov, za ketere študent še ni rešil ankete, ločeni z znakom »x« (npr. 1234x2234)
* predmeti\_reseni
  + ID-ji predmetov, za ketere je študent že rešil ankete, ločeni z znakom »x« (npr. 1234x2234)

## Preverjanje za anketo PO izpitu

http://ul.1ka.si/main/survey/studentska\_prijava2\_uni.php?fakulteta=kraticaFakultete&student=md5SifraStudenta&predmeti= idPredmeta1xidPredmeta2xidPredmeta3

Skripta vrne string v JSON formatu s polji:

* student
  + ID študenta zakodiran z md5, za katerega se izvaja preverjanje
* prijava
  + false, če se ne dovoli prijave, ker niso rešene ankete za vse predmete
  + true, če se dovoli prijava, ker so ankete za vse predmete rešene
* predmeti\_nereseni
  + ID-ji predmetov, za ketere študent še ni rešil ankete, ločeni z znakom »x« (npr. 1234x2234)
* predmeti\_reseni
  + ID-ji predmetov, za ketere je študent že rešil ankete, ločeni z znakom »x« (npr. 1234x2234)

## Preverjanje za splošno anketo

http://ul.1ka.si/main/survey/studentska\_prijava3\_uni.php?fakulteta=kraticaFakultete&student=md5SifraStudenta

Skripta vrne string v JSON formatu s polji:

* student
  + ID študenta zakodiran z md5, za katerega se izvaja preverjanje
* prijava
  + false, če se ne dovoli prijave, ker še ni rešena splošna anketa
  + true, če se dovoli prijava, ker je splošna anketa rešena

## Preverjanje za podiplomsko anketo

http://ul.1ka.si/main/survey/studentska\_prijava\_podipl\_uni.php?student=md5SifraStudenta

Skripta vrne string v JSON formatu s polji:

* student
  + ID študenta zakodiran z md5, za katerega se izvaja preverjanje
* prijava
  + false, če se ne dovoli prijave, ker še ni rešena podiplomska anketa
  + true, če se dovoli prijava, ker je podiplomska anketa rešena

## Splošno o parametrih:

* student -> ID študenta zakodiran z md5
* predmeti -> ID-ji predmetov, za katere se preverja rešenost ankete, ločeni z znakom »x« (število predmetov je poljubno)
* fakulteta -> kratica fakultete (fdv, fgg, fri...)

# Reševanje anket

* Anketo PRED izpitom morajo študenti rešiti za predmete, ki so jih vpisali / poslušali v tekočem semestru, za katere nimajo veljavne prijavnice na izpit, nimajo vpisane končne ocene in nimajo zapisnika za priznanje izpita. Kontrola: pred prijavo na izpt
* Anketo PO izpitu morajo študenti rešiti za predmete, katere so poslušali in pri katerih so pridobili končno oceno v tekočem študijskem letu ter zanje nimajo zapisnika za priznanje izpita. Kontrola: pred prijavo na izpit in pred vnosom vpisnega lista
* Splošna anketa… Kontrola: pred vnosom vpisnega lista

Ankete lahko izpolnjujejo vsi študenti 1. in 2. stopnje s statusom; študenti brez statusa, občani in študenti na izmenjavi anket zaenkrat ne izpolnjujejo.