

## İSİM

crypt – parola ve veri şifrelemesi

## BİLDİRİM

```
#define _XOPEN_SOURCE
#include <unistd.h>
```

```
void crypt (const char *parola, const char *tuz);
```

**-lcrypt** ile ilintileme gerektirir.

## AÇIKLAMA

**crypt** parola şifreleme işlevidir. Veri Şifreleme Standartı (Data Encryption Standard) algoritmasına dayanır, fakat anahtar tarama için tasarlanmış donanımlara engel olmak için bir takım farklılıklar içerir.

*parola* kullanıcın girdiği paroladır.

*tuz* ise, elemanları [a-zA-Z0-9./] kümesinden seçilen iki karakterli bir dizgedir. Bu dizge algoritmayı 4096 farklı ihtimalden biri ile karıştırmayı amaçlar.

*parolanın* ilk sekiz karakterinden her birinin en düşük anlamlı 7 biti alınarak 56 bitlik parola oluşturulur. Bu 56 bitlik parola tekrar tekrar bir dizgeyi (genellikle hepsi sıfırlardan oluşan bir dizge) şifrelemede kullanılır. Dönüş değeri 13 karakterli bir ASCII dizgesi olan ve ilk iki karakteri tuzu temsil eden şifrelenmiş paroladır. Dönüş değeri, her işlev çağrısında içeriği değişen statik bir veridir.



### Uyarı

Anahtar aralığı  $2^{56}$  (7.2e16) farklı değer içermektedir. Bu anahtar aralığının tümünü kapsayan taramalar paralel bilgisayarlar ile mümkündür. **crack(1)** gibi yazılımlar bu anahtar aralığının bir kısmını tarayıp parolaları elde etmek için insanlar tarafından kullanılmaktadır. Bu sebeple, parola seçerken sık kullanılan kelime ve isimlerden sakınılmalıdır. Parola seçme işlemi esnasında kırılabilir parolaları kontrol eden **passwd(1)** uygulaması kullanılmalıdır.

DES algoritması, **crypt** arayüzünün parola kimlik denetimi haricinde kullanılmasını kötü bir seçenek haline getirmiştir. Eğer **crypt** arayüzünü kriptografi projenizde kullanmayı planlıyorsanız, bundan vazgeçin: Şifreleme ve DES kütüphaneleri konusunda iyi bir kitap elde edinin.

## DÖNÜŞ DEĞERİ

Dönüş değeri şifrelenmiş parolaya bir göstericidir. Hata durumunda, boş gösterici döner.

## HATALAR

### ENOSYS

İşlev kütüphanede bulunmamaktadır (Örneğin, ABD'nin ihracat sınırlamalarından dolayı).

## GNU OLUŞUMU

Bu işlevin glibc2 sürümü şu ek özelliklere sahiptir. Eğer *tuz* karakter dizisi, "\$1\$" karakterleri ile başlar ve bunun ardından en fazla 8 karakter gelirse (ve tercihan "\$" karakteri ile sonlandırılırsa), bu durumda glib crypt işlevi DES motoru yerine, MD5 algoritması kullanılır ve 34 bayta kadar çıktı verilir. Çıktı "\$1\$<dizge>\$" biçimindedir. Burada *dizge*, 8 karaktere kadar *tuz* ve bunu takip eden [a-zA-Z0-9./] kümesinden seçilmiş 22 bayttan oluşur. Burada bu anahtarın bütünü anlamlıdır (sadece ilk 8 baytı değil).

Bu işlevin kullanıldığı yazılımlar derlenirken **-lcrypt** ile ilintilemelidir.

## UYUMLULUK

**crypt()** işlevi SVID, X/OPEN, BSD 4.3 ve POSIX 1003.1–2001 uyumludur.

## İLGİLİ BELGELER

**login(1)**, **crypt(1)**, **passwd(1)**, **encrypt(3)**, **getpass(3)**, **passwd(5)**.

## ÇEVİREN

Emin İslam Tatlı <[eminislam@web.de](mailto:eminislam@web.de)>, Nisan 2004

## YASAL UYARI

Bu çevirinin telif hakkı yukarıda belirtilen çevirmen(ler)e aittir. Özgün belgenin telif hakkı ve lisans bilgileri varsa ve belge içinde belirtilmemişse belge sonunda belirtilmiş olacaktır. Bu çevirinin lisansı, özgün belge için belirtilmiş bir lisans varsa ve bu lisans çevirinin de aynı lisansa sahip olmasını gerektiriyorsa onunla aynıdır, yoksa GNU GPL lisansı ve her iki durumda da ek olarak aşağıdaki koşullar geçerlidir. GNU GPL lisansı <<http://www.gnu.org/licenses/gpl.html>> adresinden edinilebilir.

BU BELGE ÜCRETSİZ OLARAK RUHSATLANDIĞI İÇİN, BELGENİN İÇERDİĞİ BİLGİLERİN VEYA KODLARIN NİTELİKLERİ İÇİN İLGİLİ KANUNLARIN İZİN VERDİĞİ ÖLÇÜDE HERHANGİ BİR GARANTİ VERİLMEMEKTEDİR. AKSİ YAZILI OLARAK BELİRTİLMEDİĞİ MÜDDETÇE TELİF HAKKI SAHİPLERİ VE/VEYA BAŞKA ŞAHISLAR BELGELERİ "OLDUĞU GİBİ", AŞIKAR VEYA ZİMNEN, SATILABİLİRLİĞİ VEYA HERHANGİ BİR AMACA UYGUNLUĞU DA DAHİL OLMAK ÜZERE HİÇBİR GARANTİ VERMEKSİZİN DAĞITMAKTADIRLAR. BELGELERİN KALİTESİ VEYA PERFORMANSI İLE İLGİLİ TÜM SORUNLAR SİZE AİTTİR. HERHANGİ BİR HATA VEYA EKSİKLİKTEN DOLAYI DOĞABİLECEK OLAN BÜTÜN SERVİS, TAMİR VEYA DÜZELTME MASRAFLARI SİZE AİTTİR.

İLGİLİ KANUNUN İCBAR ETTİĞİ DURUMLAR VEYA YAZILI ANLAŞMA HARİCİNDE HERHANGİ BİR ŞEKİLDE TELİF HAKKI SAHİBİ VEYA YUKARIDA İZİN VERİLDİĞİ ŞEKİLDE BELGEYİ DEĞİŞTİREN VEYA YENİDEN DAĞITAN HERHANGİ BİR KİŞİ, BELGENİN İÇERDİĞİ BİLGİNİN KULLANIMI VEYA KULLANILAMAMASI (VEYA VERİ KAYBI OLUŞMASI, VERİNİN YANLIŞ HALE GELMESİ, SİZİN VEYA ÜÇÜNCÜ ŞAHISLARIN ZARARA UĞRAMASI VEYA BİLGİNİN BAŞKA BİLGİLERLE UYUMSUZ OLMASI) YÜZÜNDEN OLUŞAN GENEL, ÖZEL, DOĞRUDAN YA DA DOLAYLI HERHANGİ BİR ZARARDAN, BÖYLE BİR TAZMİNAT TALEBİ TELİF HAKKI SAHİBİ VEYA İLGİLİ KİŞİYE BİLDİRİLMİŞ OLSA DAHİ, SORUMLU DEĞİLDİR.

## Özgün belgedeki telif hakkı beyanı

Michael Haardt ([michael@cantor.informatik.rwth.aachen.de](mailto:michael@cantor.informatik.rwth.aachen.de)) Sat Sep 3 22:00:30 MET DST 1994

This is free documentation; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

The GNU General Public License's references to "object code" and "executables" are to be interpreted as the output of any document formatting or typesetting system, including intermediate and printed output.

This manual is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this manual; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111, USA.

Sun Feb 19 21:32:25 1995, faith@cs.unc.edu edited details away

TO DO: This manual page should go more into detail how DES is perturbed, which string will be encrypted, and what determines the repetition factor. Is a simple repetition using ECB used, or something more advanced? I hope the presented explanations are at least better than nothing, but by no means enough.

added \_XOPEN\_SOURCE, aeb, 970705  
added GNU MD5 stuff, aeb, 011223

---

23 Aralık 2001

crypt(3)

Bu dosya (man3-crypt.pdf), belgenin XML biçiminin T<sub>E</sub>XLive ve belgeler-xsl paketlerindeki araçlar kullanılarak PDF biçimine dönüştürülmesiyle elde edilmiştir.

19 Ocak 2007