

# Spring Security Crypto Modülü



# Crypto Modülü

- Spring Security **core içerisinde** yer alır
- Çalışması için herhangi bir **security veya Spring konfigürasyonuna ihtiyaç duyulmaz**
- Aşağıdaki **kabiliyetleri** içerir
  - Password encoding
  - Symmetric encryption
  - Key üretimi

# Encryptors

```
Encryptors.standard("password", "salt");
```

PKCS #5's PBKDF2 (Password-Based Key Derivation Function #2) kullanarak 256-bit AES üretir  
 SecretKey üretmek için kullanılan password gizli kalmalı ve paylaşılmamalıdır  
 Salt değeri hex-encoded String form'da, random, ve en az 8 byte olmalıdır

```
String salt = KeyGenerators.string().generateKey();
```

```
Encryptors.text("password", "salt");
```

Text veriyi BytesEncryptor kullanarak encrypt eder ve kolay saklanabilmesi için hex-encoded string çıktı üretir

```
Encryptors.queryableText("password", "salt");
```

# Key Generators

```
BytesKeyGenerator generator =  
    KeyGenerators.secureRandom();
```

```
byte[] key = generator.generateKey();
```

```
KeyGenerators.secureRandom(16);
```

```
KeyGenerators.shared(16);
```

```
KeyGenerators.string();
```

# Password Encoding

```
BCryptPasswordEncoder encoder =  
    new BCryptPasswordEncoder(16);
```

```
String result = encoder.encode("myPassword");
```

```
encoder.matches("myPassword", result);
```

# İletişim

- **Harezmi** Bilişim Çözümleri
- Kurumsal Java Eğitimleri
- <http://www.java-egitimleri.com>
- [info@java-egitimleri.com](mailto:info@java-egitimleri.com)

