**AMAÇ :** Bu uygulamanın amacı kişiye kriptoloji biliminde açık metin ile şifreli metin arasındaki bağı azaltmak için kullanılan çığ etkisi prensibinin uygulamadaki örneklerini göstermektir.

**ÖNBİLGİ :**

Bir şifreleme algoritmasında anahtar veya şifresiz metindeki küçük değişikliklerin şifreli metin üzerinde büyük değişikliğe neden olmasına çığ (avalance) etkisi denir.

**UYGULAMA :**

1. **Uygulama öncesi yapılacaklar :**

* sudo apt-get install openssl komutuyla şifreleme uygulamasını kurun.
* sudo apt-get install base64 komutuyla encodimg uygulamasını kurun.

1. **Uygulamanın Yapılışı:**
2. Avalanche\_affects.py programı üzerinden açık metinde küçük değişiklikler yaparak şifreli metinde meydana gelen değişimleri gözlemleyin.
3. Programda kullanılan anahtar ve metni değiştirerek programı çalıştırıp sonuçları gözlemleyin.
4. echo “gizli bilgi” |base64 ve echo “izli bilgi” |base64 komutlarını çalıştırarak çıktılar arasındaki farkı gözlemleyin.
5. Yukarıdaki programda bulunan fonksiyonu aes algoritması için yazıp sonuçlarını gözlemleyin.

**ANALİZ :**

* DES ve base64 algoritmalarının çiğ etkisine tepkisni tartışın
* DES algoritmasına anahtar boyutu etkisini tartışın.
* Çığ etkisi anlamında DES ve AES arasındaki fark nedir.

**REFERANSLAR :**

1 – Mehmet İnce, Crypto 101 – [2] Block Cipher Encryption ve DES Analizi, https://www.mehmetince.net/crypto-101-2-block-cipher-encryption-ve-des-analizi/