Ağ ve Bilişim Güvenliği

Öğr. Gör. Zafer SERİN

KRİPTOGRAFİK TERİMLER

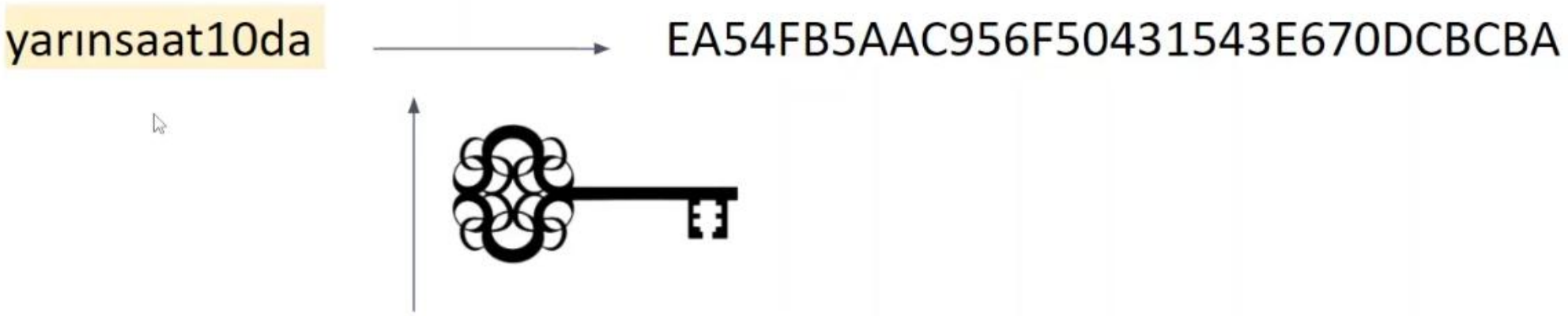
- **Anahtar(Key)**

1. Anahtar bir kripto sistemin en önemli parçalarından birisidir.
2. Gizlilik tamamen anahtarın gizliliğine dayalıdır.
3. Simetrik şifreleme de aynı anahtar ile şifreleme ve deşifre işlemleri yapılırken asimetrik şifrelemede şifreleme için kullanılan anahtar ve deşifreleme için kullanılan anahtar farklıdır.
4. Anahtarların bitsel olarak uzun ve karmaşık olması gerekir.
5. Günümüz bilgisayarları 70 bite kadar işlemleri yapabilmektedir. Bu nedenle anahtarın en azından 80 bit olması tercih edilmelidir.

KRİPTOGRAFİK TERİMLER

- **Açık Metin(Plain Text)**

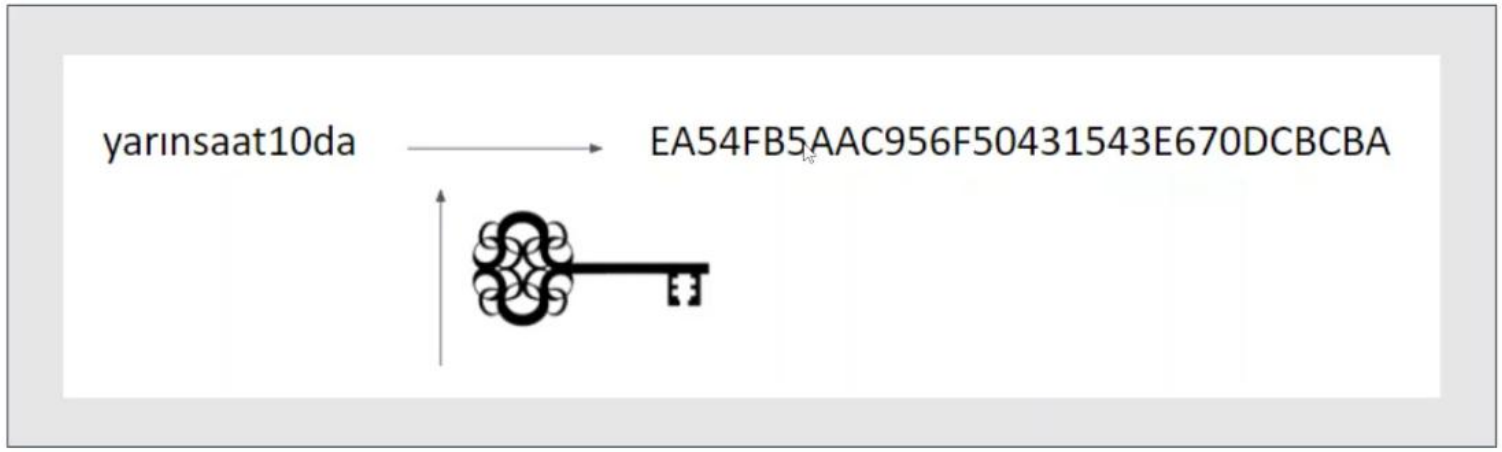
1. Şifrelenecek metini ifade etmektedir.
2. Entropisi şifrelenmiş metine göre daha düşüktür.
3. Kayıpsız olarak sıkıştırmaya uygundur.



KRİPTOGRAFİK TERİMLER

- **Şifreleme(Encyrption)**

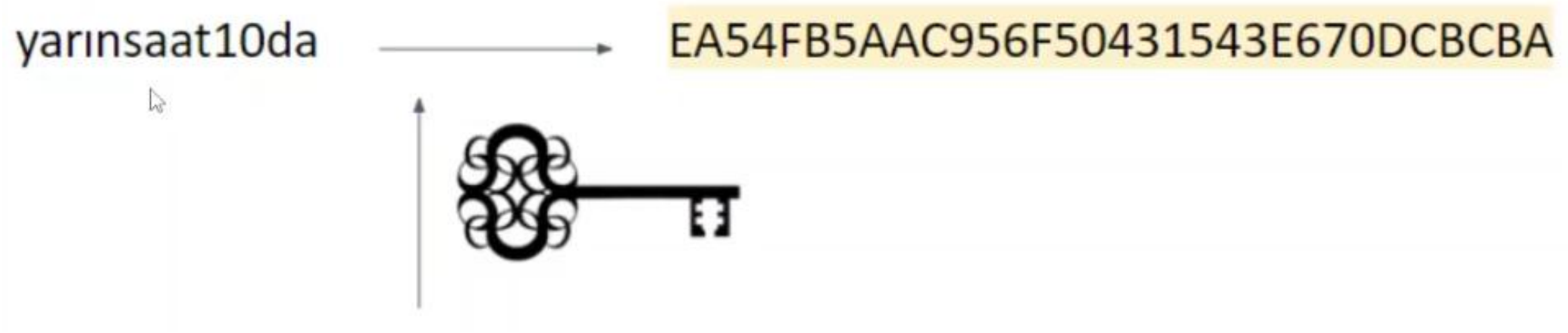
1. Şifreleme ilgili verinin veya bilginin alternatif bir forma dönüştürülmesidir.



KRİPTOGRAFİK TERİMLER

- **Şifreli Metin(Cipher Text)**

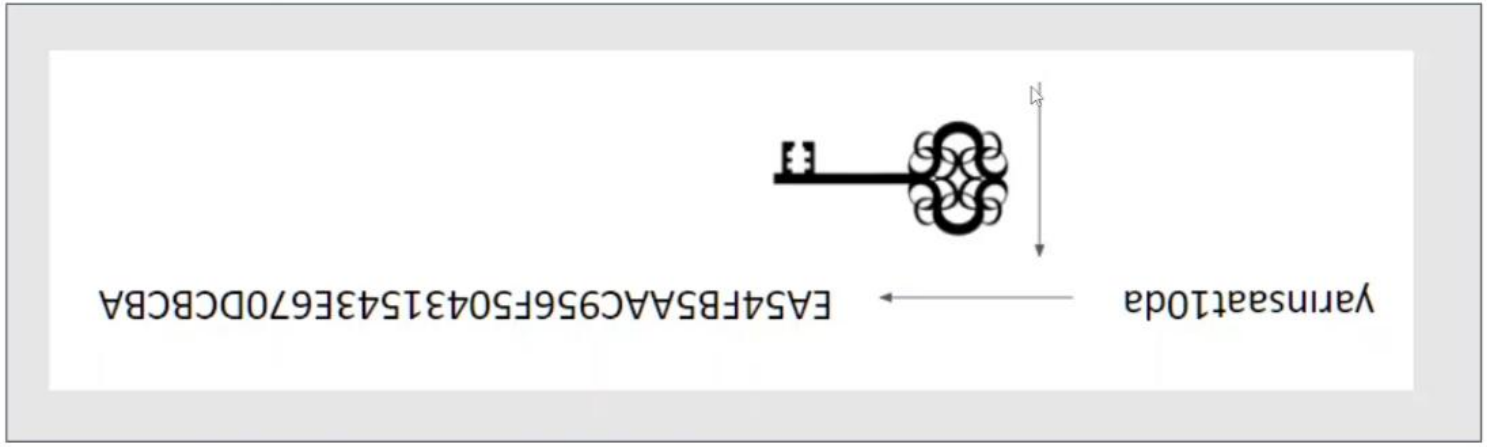
1. Şifreli Metin ilgili bilgi veya verinin alternatif forma dönüştürülmüş halidir.



KRİPTOGRAFİK TERİMLER

- **Deşifreleme(Decryption)**

1. Şifreleme işleminin tersini ifade eder.
2. Deşifreleme şifrelenmiş yapının ilk haline döndürülmesi işlemidir.



KRİPTOGRAFİK TERİMLER

- **Güvenlik Seviyesi(Bit cinsinden)**

1. Saldırı bir kriptosisteme deneme-yanılma dışında yapılacak her türlü işlemi ifade eder.
2. RSA3072 3072 adet bit içerir ve deneme-yanılma ile buna erişilebilir; ancak eğer deneme-yanılma ile değilde saldırı ile çeşitli matematiksel denemeler ve asal çarpanlara ayırma gibi işlemler yapılırsa elimizde RSA3072'yi deneme-yanılma ile kırabilecek 128 bit kalır. Bu durumda RSA3072'nin güvenlik seviyesi 128 bittir denilebilir.

KRİPTOGRAFİK TERİMLER

- **Güvenlik Seviyesi(Bit cinsinden)**

3. Buna karşın AES128'e herhangi bir saldırı yapılamadığı ve matematiksel olarak bir şey çıkarılamadığı için AES128'in güvenliğide doğrudan 128 bittir denilir.
4. Bu durumda AES128 RSA3072'ye denk sayılabilir.

KRİPTOGRAFİK TERİMLER

Security (Bits)	Symmetric encryption algorithm	Minimum Size (Bits) of Public Keys		
		DSA/DH	RSA	ECC
80	Skipjack	1024	1024	160
112	3DES	2048	2048	224
128	AES-128	3072	3072	256
192	AES-192	7680	7680	384
256	AES-256	15360	15360	512

KRİPTOGRAFİK TERİMLER

- **Kriptosistem**

1. Şifreleme ve Deşifrelemeden meydana gelen sistemdir.
2. Şifreleme + Deşifreleme = Kriptosistem

KRİPTOGRANİN TEMEL KURALLARI

- **Kural 1: Kerckhoffs Prensibi**

1. Anahtar ne olursa olsun gizli kalmalıdır. Anahtar dışında kalanlara herkes tarafından erişilebilir.
2. Enigma ve günümüzün en iyi şifreleme algoritmalarından AES bu prensibe uymaktadır.

KRİPTOGRANİN TEMEL KURALLARI

- **Kural 2: Kendin bir Algoritma Üretme**

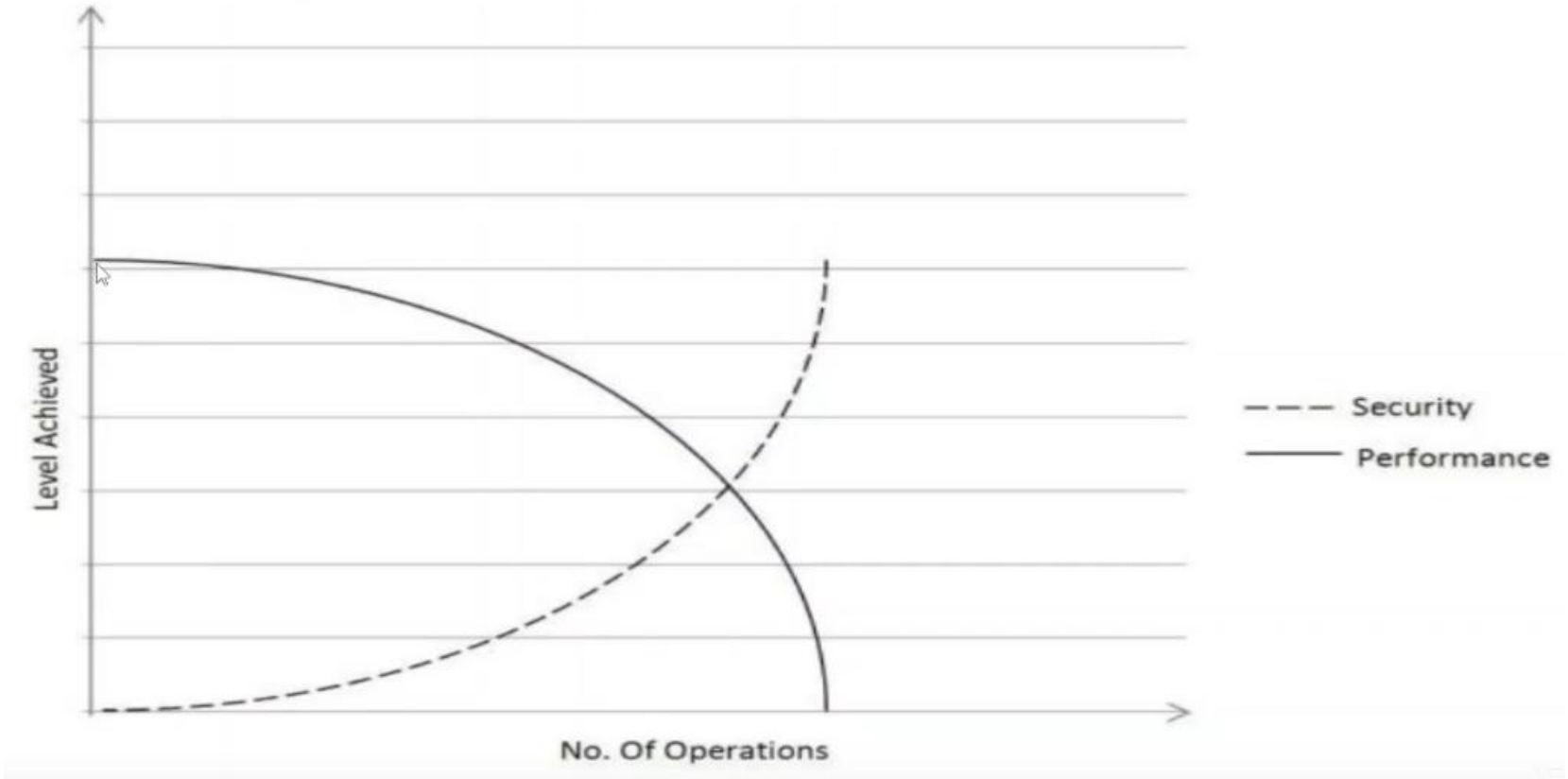
1. Bir şifreleme algoritmasının güvenli, hızlı ve matematiksel olarak ispatının yapılması gerekir.
2. Ufak bir grup tarafından geliştirilen algoritma çok fazla insana ulaşamayabilir ve bu durumda pek çok farklı kişi tarafından test edilmesi mümkün olmayabilir. Bu durum şifreleme ile taban tabana zıt düşer.
3. NIST kimi zamanlar bazı yarışlar açarak yeni geliştirilen şifreleme algoritmalarının herkes tarafından denenmesini sağlar.

KRİPTOGRANİN TEMEL KURALLARI

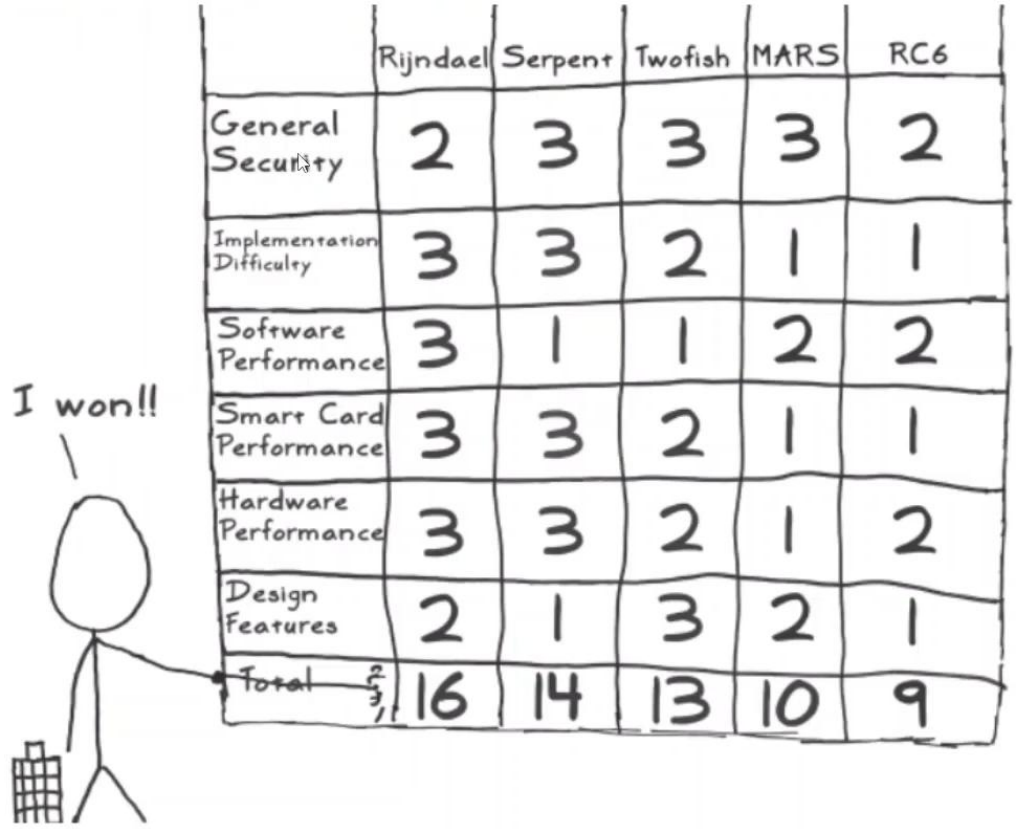
- **Kural 3: En Güvenli En İyi Değildir**

1. Burada temel amacın iletişim olduğu unutulmamalıdır. İletişimi kesecek derecede güvenlik sağlamak bir anlam ifade etmeyecektir.
2. Veriyi şifreleyerek göndermek şifrelemeden göndermeye nazaran daima daha maliyetli olacaktır.

KRİPTOGRANİN TEMEL KURALLARI



KRİPTOGRANİN TEMEL KURALLARI



	Rijndael	Serpent	Twofish	MARS	RC6
General Security	2	3	3	3	2
Implementation Difficulty	3	3	2	1	1
Software Performance	3	1	1	2	2
Smart Card Performance	3	3	2	1	1
Hardware Performance	3	3	2	1	2
Design Features	2	1	3	2	1
~~Total~~	16	14	13	10	9