



# RFID TEKNOLOJİSİ -Ve Güvenliği-



~ RFID Nedir?

## **Radio Frequency IDentification**

# ~ RFID Nedir?

Nesneleri radyo frekansı aracılığı ile tekil ve otomatik olarak temassız bir şekilde tanıtmaya yarayan Radyo Frekanslı Tanıma (RFID) teknolojisi günümüzde mobil ve kablosuz iletişim teknolojileri içerisinde kendisine önemli bir yer edinmiştir.

Geçmişte eski de olsa, yarı iletken teknolojisindeki gelişmeler ve maliyetlerin azalması ile bu teknoloji, farklı endüstrilerde süreçlerin etkinliğini arttırdığından ve kullanıcılarla günlük hayatta ciddi fayda ve kolaylıklar sağladığından kitlesel uygulamalarda sıkça kullanılmaktadır.



# ~ RFID Kullanım Alanları

- Ödeme sistemleri
- Toplu taşıma
- Otomobil kontak sistemleri
- Envanter kontrolü
- Elektronik geçiş sistemleri
- Hayvan takibi
- Personel mesai takibi

# ~ Çeşitli RFID Formları



# ~ RFID İmplant



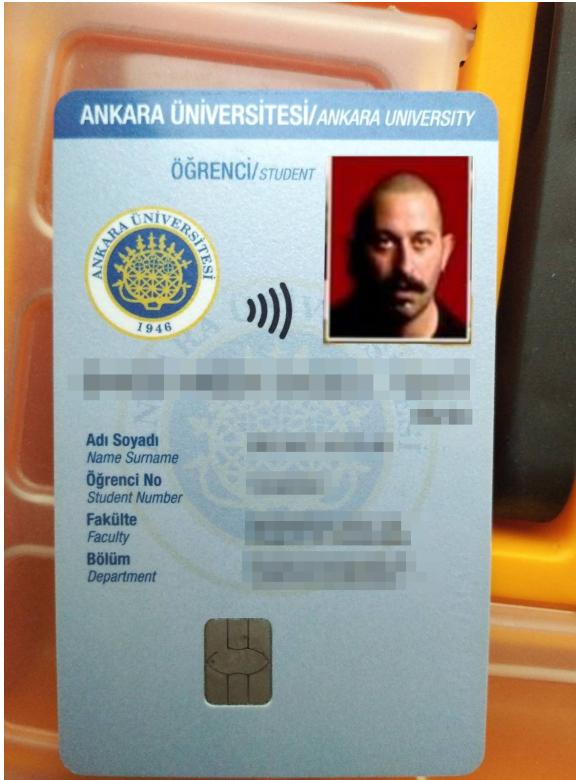
# ~ RFID Çeşitleri

	LOW-FREQUENCY (RFID)	HIGH-FREQUENCY (HF)	ULTRA-HIGH-FREQUENCY (UHF)
FREQUENCY RANGE	30 to 300 KHz	3 to 30 MHz	300 MHz to 3GHz
COMMON FREQUENCY	125 KHz or 134 KHz	13.56 MHz (NFC)	860 to 960 MHz (UHF Gen2)
RELATIVE COST	\$\$	\$\$ – \$\$\$	\$
READ RANGE	≤10 cm	≤30 cm	≤100 m
BENEFITS	More resistant to interference by liquids and metals.	Higher memory capabilities, NFC tags can function as both reader and tag.	Lower cost, with good read range and fast read rates.
COMMON APPLICATIONS	Animal tracking, automobile inventorying.	Promotional packaging and labels, contactless payment, library collections.	Inventory control, item-level tracking, supply chain visibility and efficiency.

# ~ Low-Frequency (LF)



# ~ High-Frequency (HF)



# ~ Ultra-High-Frequency (UHF)



# ~ MIFARE Classic 1 KB



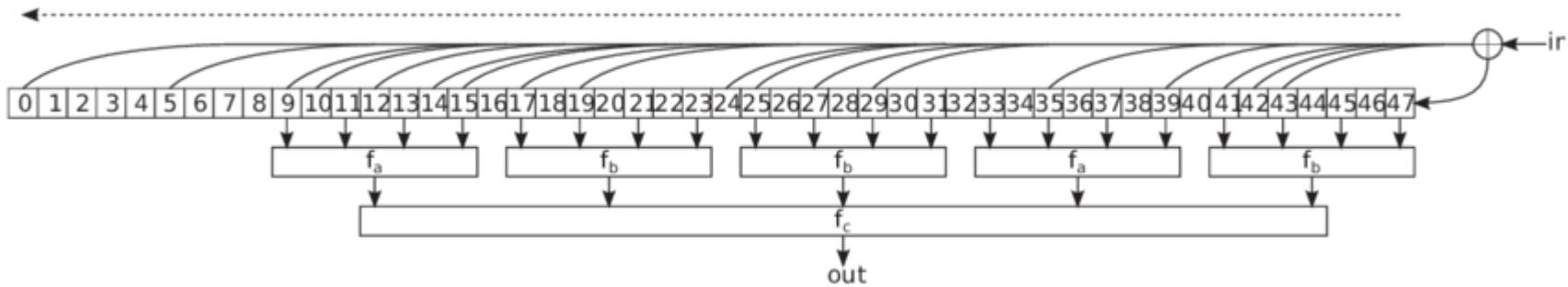
# ~ MIFARE Classic 1 KB

- NXP Semiconductors tarafından geliştirilmiştir
- En çok kullanılan NFC teknolojisi
- 10 milyarın üzerinde kart ve 150 milyonun üzerinde okuyucu üretilmiştir

# ~ MIFARE Classic 1 KB

- 13.56 MHz (HF)
- Crypto-1 isimli bir şifreleme algoritması kullanıyor
- 2008 yılında mikroskopla incelenerek Cryptow-1 algoritması açığa çıkarıldı

# ~ Crypto-1



Crypto-1 stream cipher

# ~ Crypto-1

$$L := x_0 \oplus x_5 \oplus x_9 \oplus x_{10} \oplus x_{12} \oplus x_{14} \oplus x_{15} \oplus x_{17} \oplus$$

$$x_{19} \oplus x_{24} \oplus x_{25} \oplus x_{27} \oplus x_{29} \oplus x_{35} \oplus x_{39} \oplus x_{41} \oplus x_{42} \oplus x_{43}$$

$$f_a(y_0, y_1, y_2, y_3) := ((y_0 \vee y_1) \oplus (y_0 \wedge y_3)) \oplus (y_2 \wedge ((y_0 \oplus y_1) \vee y_3))$$

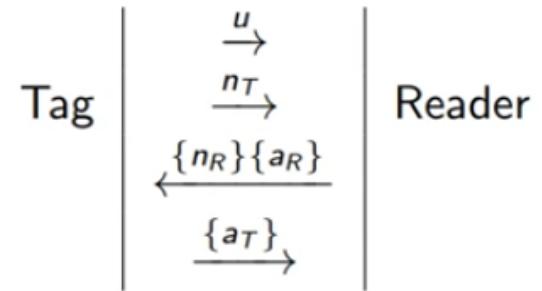
$$f_b(y_0, y_1, y_2, y_3) := ((y_0 \wedge y_1) \vee y_2) \oplus ((y_0 \oplus y_1) \wedge (y_2 \vee y_3))$$

$$f_c(y_0, y_1, y_2, y_3, y_4) := (y_0 \vee ((y_1 \vee y_4) \wedge (y_3 \oplus y_4))) \oplus ((y_0 \oplus (y_1 \wedge y_3)) \wedge ((y_2 \oplus y_3) \vee (y_1 \wedge y_4)))$$

$$suc(x_0 x_1 \dots x_{31}) := x_1 x_2 \dots x_{31} || (x_{16} \oplus x_{18} \oplus x_{19} \oplus x_{21})$$

# ~ Kimlik Doğrulama Süreci

- 1- Kart, uid'sini okuyucuya gönderir
- 2- Okuyucu, belli bir sektörü okumak için istek atar
- 3- Kart, bir challenge gönderir
- 4- Okuyucu, kartın cevabını ve kendi challenge'ını gönderir
- 5- Son olarak kart , okuyucunun cevabını gönderir



## ~ Zafiyet

- Karta gönderilen cipher text için ilk 8 bit doğru fakat kalanı yanlışsa kart okuyucuya error gönderir
- Error message: hex(5)
- Bu sayede key'in 4 biti sızmış oluyor



## ~ Bilinen Zayıflıkları

- Zayıf PRNG
- Kısa boyutlu key
- Error'da bit sızması
- Parity bit
- İç içe kimlik doğrulama

# ~ Online Saldırılar

Attack	Traces	Gather	Compute	<sup>a</sup>	<sup>b</sup>
(Garcia et al., 2009)	2	<1 sec	<1 sec	✗	✓
(Courtois, 2009)	300	3 min	<1 sec	✗	✗
(Chiu et al., 2013)	~ 100,000	10-20 hours	2-15 min	✓	✗
(Meijer and Verdult, 2015)	~ 10,000	6-12 min	5-10 min	✓	✓

# ~ Offline Saldırılar

Reference	GPU	Cores	Speed	Time
(Meijer and Verdult, 2015)	GTX 460	336	1350 MHz	1 month

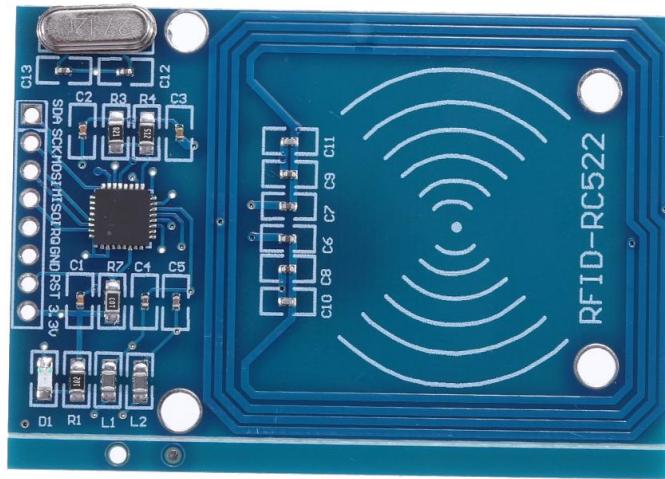
# ~ Brute Force



# ~ Uygulama Hataları

- Basit devreler
- Kimlik doğrulama için UID kullanılması

# ~ RFC522



# ~ UID Değişebilir Kartlar



UID Changeable IC

M1 S50

13.56MHz

BOŞ 13.56Mhz Kilit Sistemleri için  
UID Writable MIFARE Classic Kart. Kopyalama Cihazı

★★★★★ Yorumları oku (6)

Ürün Tercihi

Seçin

Adet

1

Kargo Ücreti : 11,90 TL

Mağazaya özel 350 TL ve üzeri Ücretsiz Kargo

En geç 15 Aralık Çarşamba günü kargoya verilir.

[Detayları gör](#)

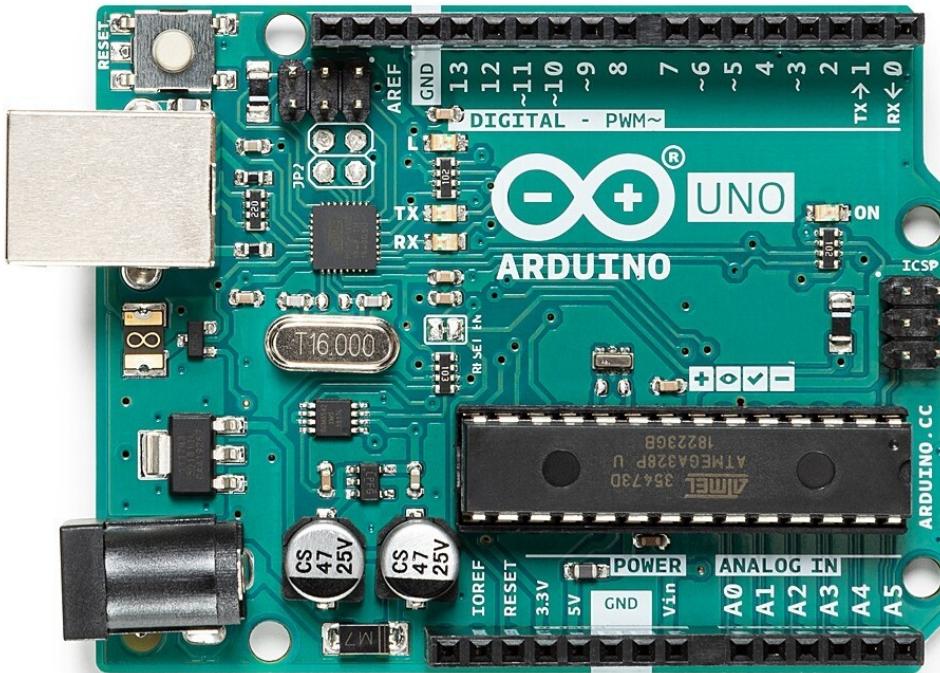
8,99 TL KDV DAHİL

Bu Mağazadan minimum 25 TL tutarında alışveriş yapabilirsiniz

Hemen AL

Sepete Ekle

# ~ Arduino





~ ./kapanis

**Teşekkürler**