

# HASH FONKSİYONLARI

BİLGİSAYAR MÜHENDİSLİĞİ

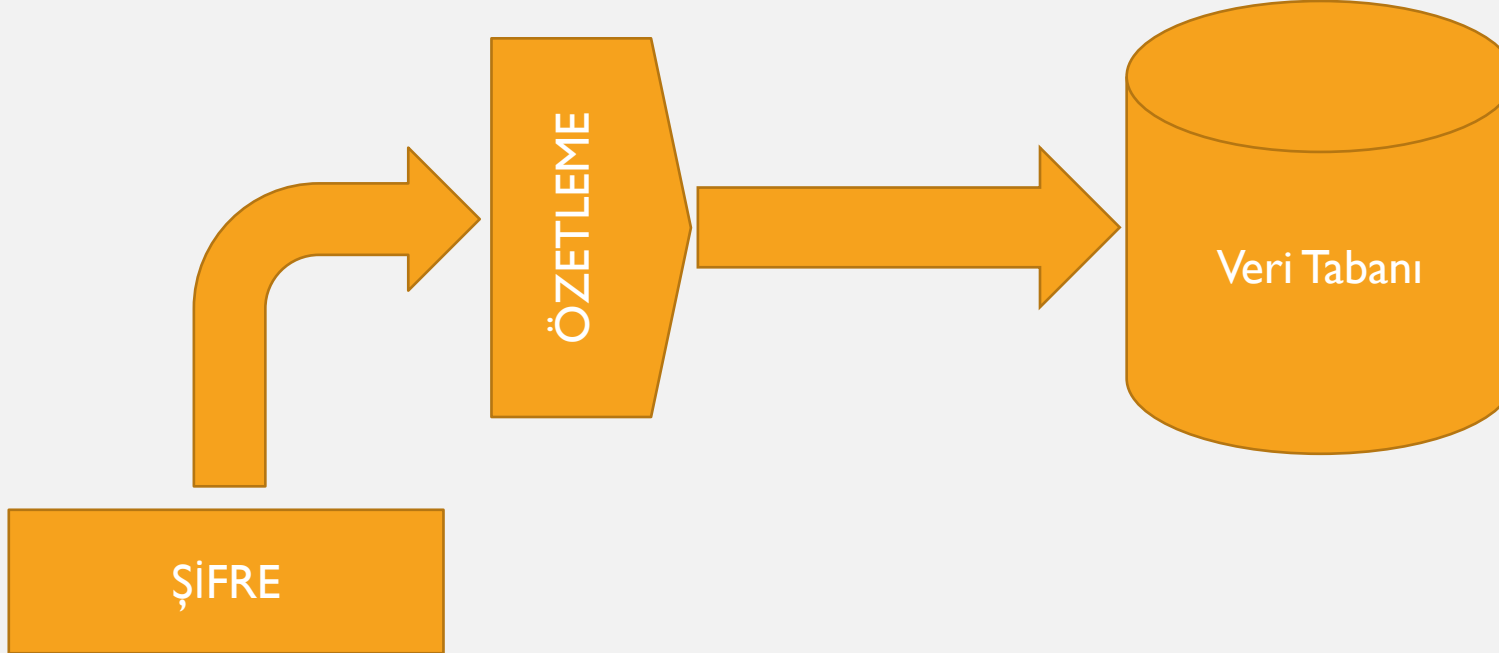
# ÖZETLEME (HASHİNG)

- **Özetleme (hashing)**, temel olarak verinin bütünlüğünü sağlamak için kullanılan bir yöntemdir.
- Alınan bir verinin boyutundan bağımsız olarak sabit uzunlukta ve alınan veriye özel üretilen çıktıdır. Yani aynı veriye her zaman aynı çıktıyı oluşturur.
- Örneğin MD5 özetleme fonksiyonu:
- **Teknoloji fakültesi**
- **Cc3f89ed96ae3edea9ce7ad3cf6a9cda -> 32 karakter 128 bit**
- **Teknoloji Fakültesi**
- **e7c319b360e2e124d066a6011c70c72a**
- **özetlerini oluşturur.**

# HASH FONKSİYONLARI

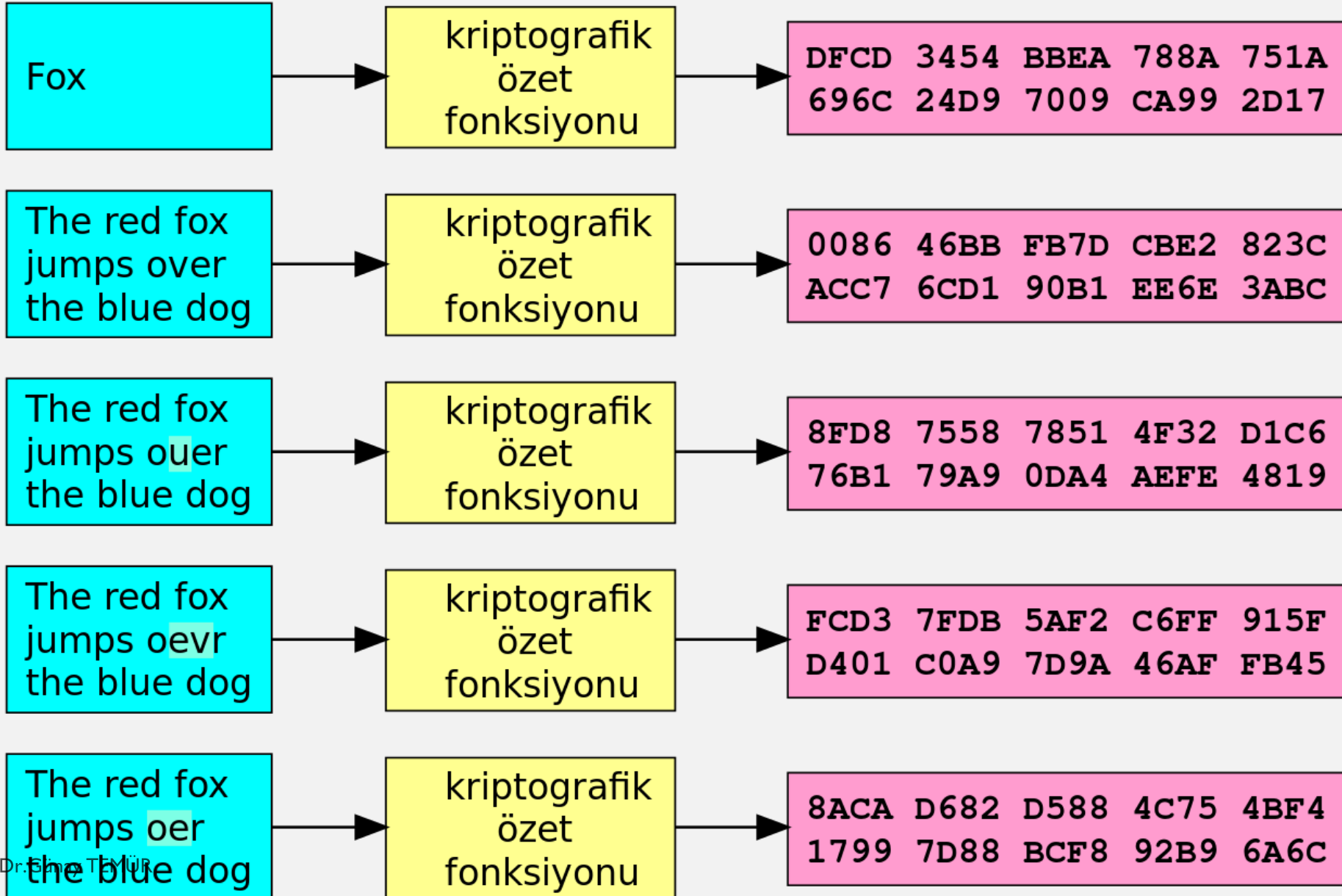
- Veritabanında Şifrelerin Tutulmasında
- Büyük Verilerde Değişiklik Olup Olmadığının Kontrolünde
- E-posta Şifreleme Uygulamaları
- Güvenli Uzaktan Erişim Uygulamaları
- İnternette Güvenli Şekilde Veri İndirme İşlemleri
- Gibi Çeşitli Alanlarda Kullanılır.

# HASH ÇALIŞMA MANTIĞI



## Girdi

## Özet



# ÖZELLİKLERİ

- Özetleme algoritmaları ile ilgili bazı önemli noktalar şunlardır:
- Özetleme algoritmaları için simetrik / asimetric gibi bir sınıflandırma yoktur. Özetleme algoritmaları anahtar kullanmazlar.
- Özetleme fonksiyonları, tek yönlüdür. Bu sebeple, özetlenen veriden, asıl veri elde edilemez. Geri dönüştürülemeden garanti edilebilmesi için güçlü algoritmalar kullanılmalıdır.
- Aynı metin, aynı özetleme algoritması ile işleme koyulursa her defasında aynı sonuç ortaya çıkar. Bu sebeple bütünlük kontrolü gerçekleştirilebilir.
- Güçlü bir özetleme algoritması ile metin üzerindeki küçük bir değişiklik, çıktıda büyük değişikliğe sebep olur.
- Blok uzunluğu ne kadar fazla olursa o kadar güvenilirdir.

# ZAYIFLIĞI

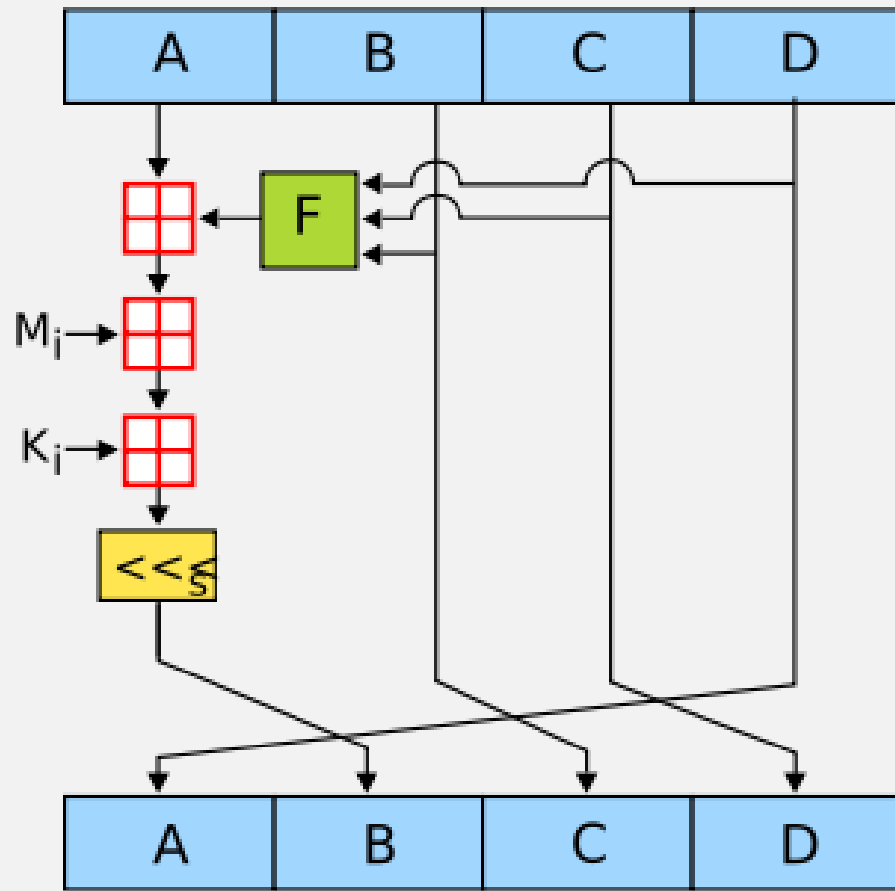
- Güvenilir bir özetleme fonksiyonunda çakışma ihtimali oldukça az olmalıdır; çakışmaya dayanıklı olmalıdır. Aksi halde özellikle kimlik doğrulama işlemlerinde zafiyet ortaya çıkar. Örneğin “Aa123456!qwerty.asdfgh?” şeklindeki karmaşık bir parolanın özeti ile “Test123” gibi bir parolanın özeti aynı çıkar ise; kaba kuvvet veya sözlük saldırıları ile deneme yapıldığında, Test123 şeklindeki bir parola ile karmaşık şekilde parola kullanan bir kişinin oturumu açılabilir. Bu istenmeyen bir durumdur.
- İki farklı girdinin aynı çıktıyı üretmesi (buna Collision=Çakışma denir) o Hash fonksiyonunu kırıldığının göstergesidir. SHA1 ve MD5 kırılan Hash fonksiyonlarına örnek olarak verilebilir.

# ZAYIFLIK TESTİ

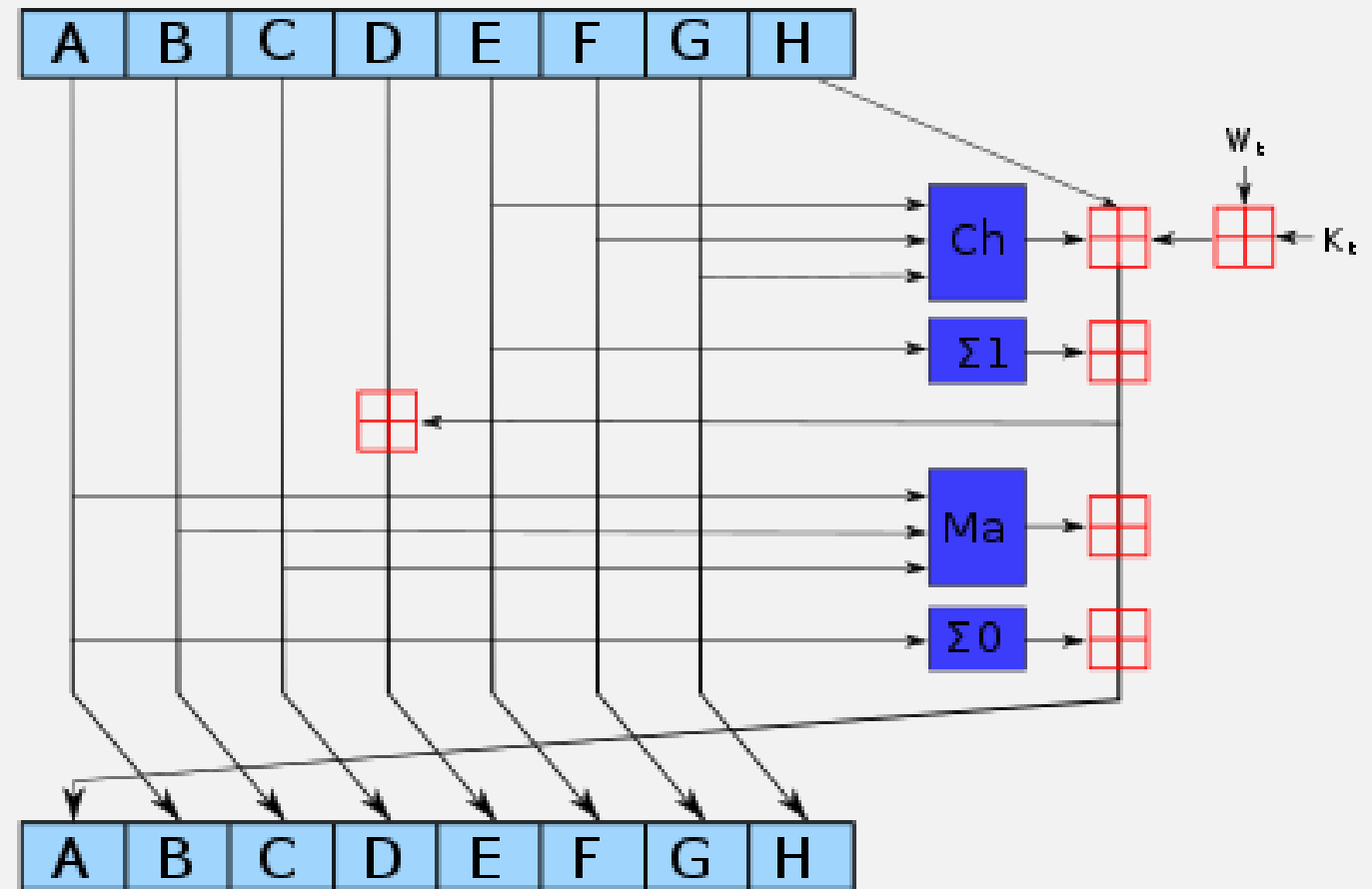
- Teknik özellikler dışında SHA1 den bahsedecek olursak; Kriptanalistlerin 2005'te yaptığı bir saldırıyla SHA1'in yeterince güvenli olmadığını ispatladılar. Bu yüzden 2010' dan beri SHA1 yerine daha güvenli olan SHA2 ailesi kullanılmaya başlandı.
- Microsoft, Google, Apple ve Mozilla SSL Sertifikalarından 2017 itibarıyla SHA1 desteğini çekeceklerini açıkladılar. Daha sonra ise Google SHA1' e çakışma saldırısı yaptıklarını ve iki farklı PDF dosyasından aynı SHA1 özet çıktığı aldıklarını ispatlayarak SHA1 in kırıldığını duyurdular.



<b>Algoritma</b>	<b>Özet boyutu (bit)</b>
GOST	256
HAVAL	256/224/192/160/128
MD2	128
MD4	128
MD5	128
PANAMA	256
RadioGatún	608/1216'ya kadar (19 kelime)
RIPEMD	128
RIPEMD-128/256	128/256
RIPEMD-160/320	160/320
SHA-0	160
SHA-1	160
SHA-256/224	256/224
SHA-512/384	512/384
Tiger(2)-192/160/128	192/160/128
WHIRLPOOL	512



MD5



SHA-2