HASH FONKSİYONLARI

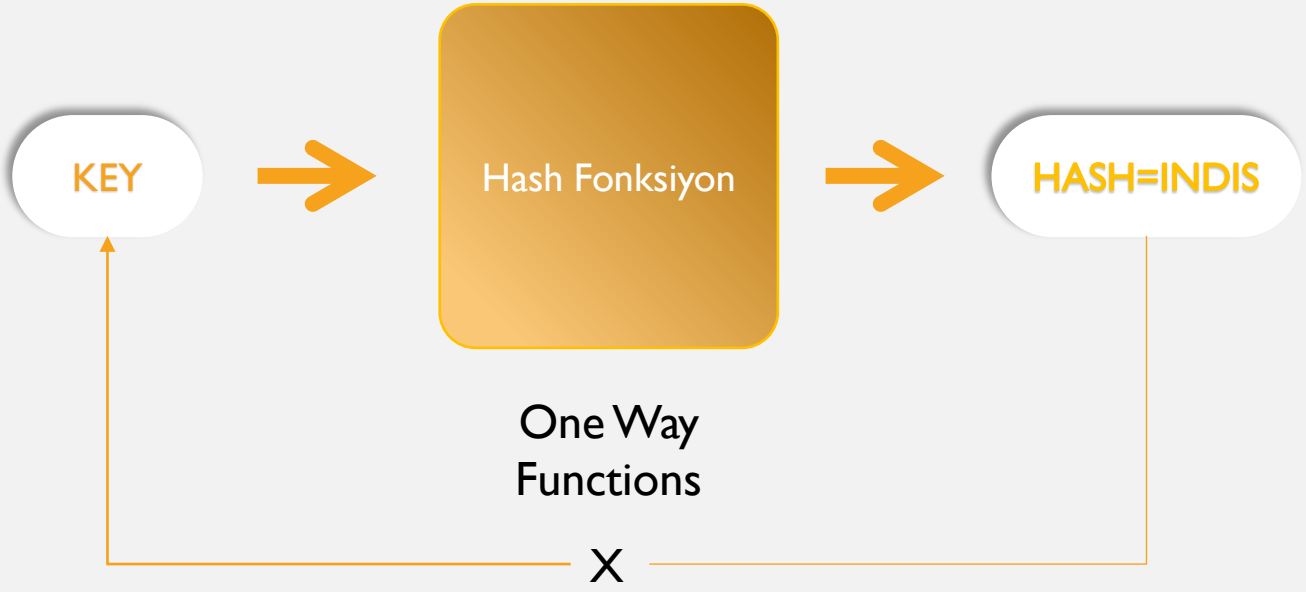
Dr. Günay TEMÜR

Hash Fonksiyonları ve Güvenlik

- Hash fonksiyonların güvenlik ve şifreleme alanında da sıkça kullanılmaktadır.
- Hash fonksiyonları tek yönlü (One Way) çalışır. Yani algoritmanın ürettiği sonuçtan **tekrar asıl metine dönüşüm** mümkün değildir.

HASH FONKSİYONLARI

- **HASH fonksiyonlarının** en iyi özellikleri **Tek yönlü** algoritmalar olmalarıdır.
- Yani: Üretilen HASH (INDIS) değerinden geri dönüşüm **mümkün değildir**.



***Hash fonksiyonları verimli bir şekilde **hesaplanabilir** olmalıdır. Gerçek uygulamalarda, algoritmamızın bir hash fonksiyonundan hash değerini hesaplaması uzun zaman alıyorsa, o zaman hashing amacını kaybederiz.

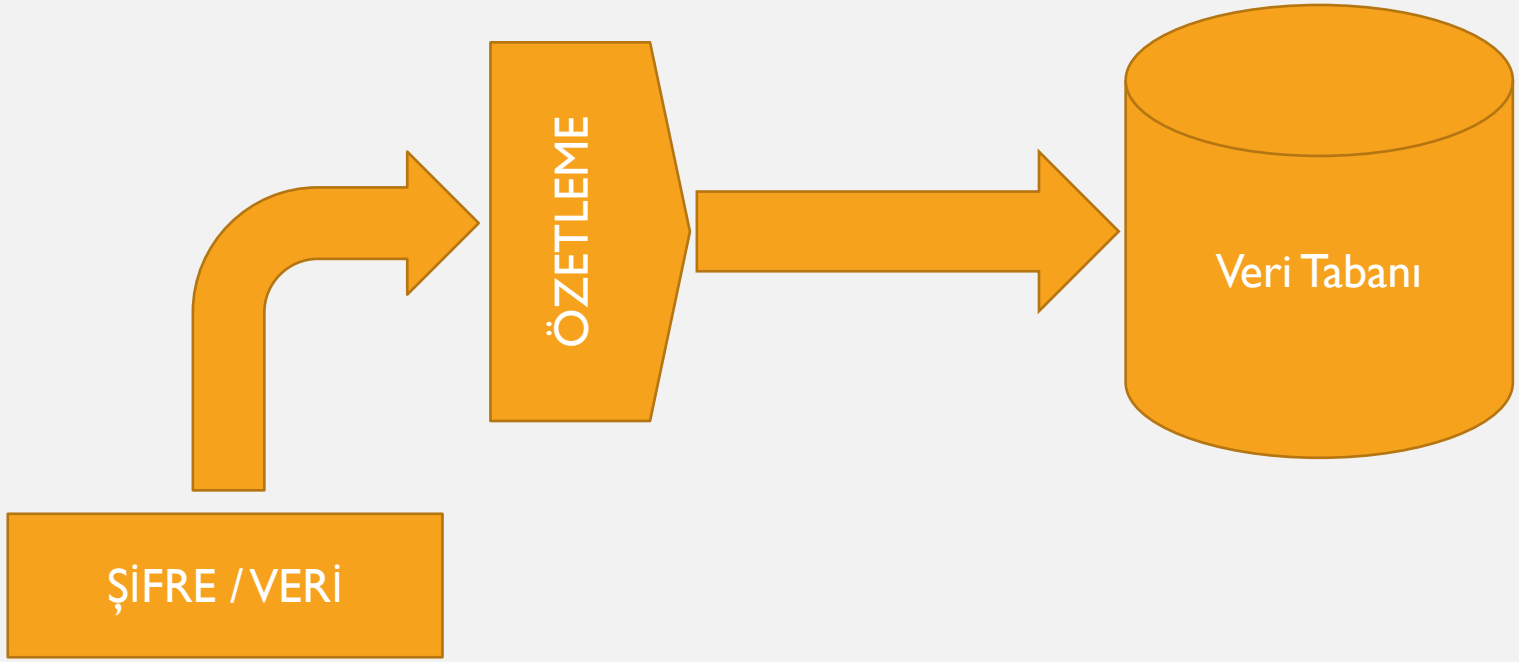
ÖZETLEME (HASHİNG)

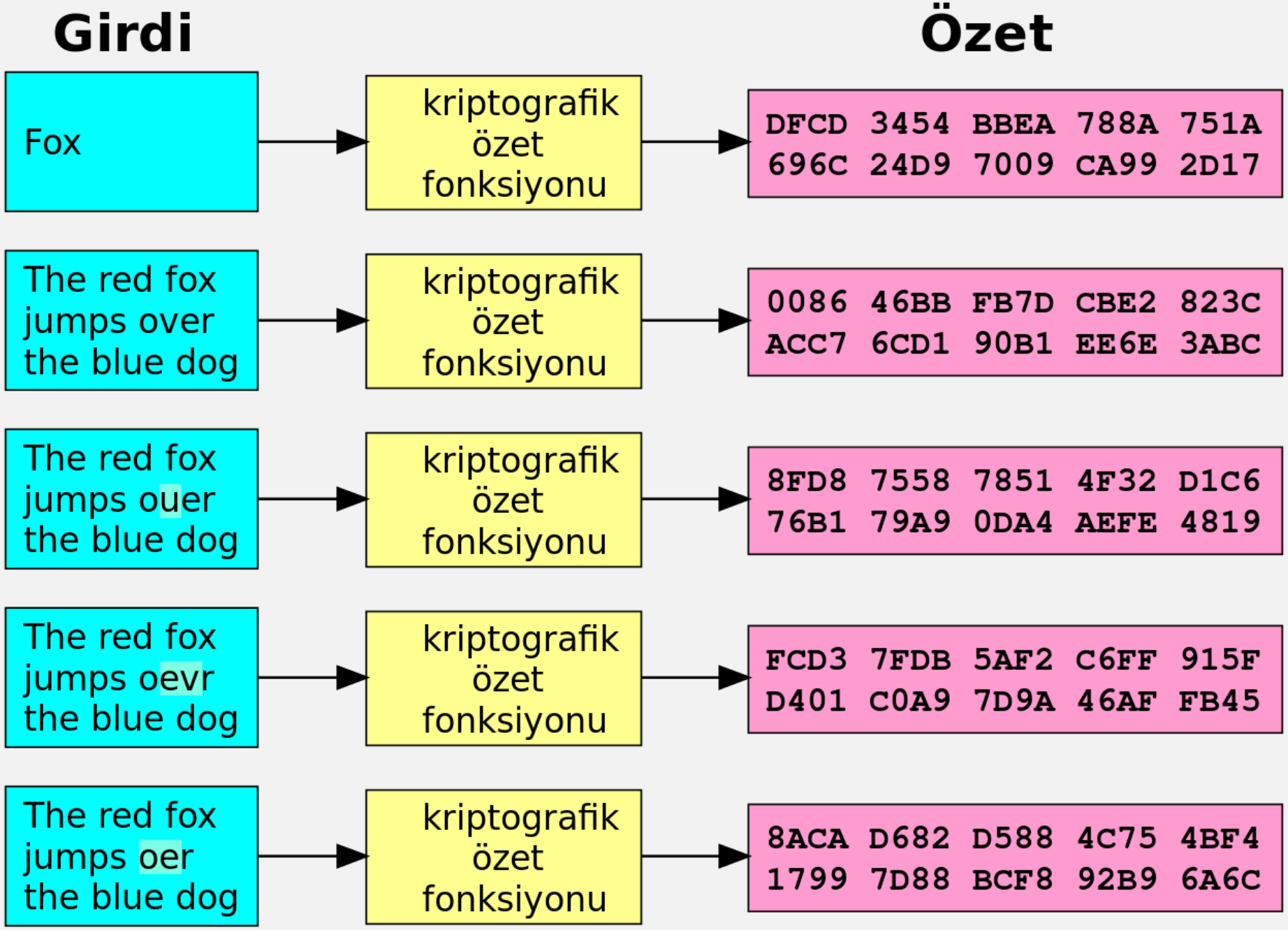
- **Özetleme (hashing)**, temel olarak verinin bütünlüğünü sağlamak için kullanılan bir yöntemdir.
- Alınan bir verinin boyutundan bağımsız olarak sabit uzunlukta ve alınan veriye özel üretilen çıktıdır. Yani aynı veriye her zaman aynı çıktıyı oluşturur.
- Örnek özetleme fonksiyon çıktıları:
- **Gölyaka MYO için**
- **3584c344f3b240f20961a117964d618f -> 32 karakter 256 bit MD5 Hash**
- **3584C344F3B240F20961A117964D618F**
- **C9bc324a27961f3f7e5eab45fcaab09fcc26aafd -> 40 karakter 320 bit SHA1 Hash**
- **Golyaka MYO için**
- **1ab5243ed57c7e83694fd483e661b928 -> MD5 Hash**
- **1AB5243ED57C7E83694FD483E661B928**
- **6BD758E5D6705B97D430F4F33AB41DB5**
- **5a43cbb2c5b53ca37f00cbcda612c122224172dd SHA1 Hash**
- **özetlerini oluşturur.**

HASH FONKSİYONLARI

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

HASH ÇALIŞMA MANTIĞI




Girdi
Özet
Fox
kriptografik özet fonksiyonu
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
kriptografik özet fonksiyonu
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
kriptografik özet fonksiyonu
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
kriptografik özet fonksiyonu
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
kriptografik özet fonksiyonu
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

ÖZELLİKLERİ

- Özetleme algoritmaları ile ilgili bazı önemli noktalar şunlardır:
- Özetleme algoritmaları için simetrik / asimetrik gibi bir sınıflandırma yoktur. Özetleme algoritmaları anahtar kullanmazlar.
- Özetleme fonksiyonları, tek yönlüdür. Bu sebeple, özetlenen veriden, asıl veri elde edilemez. Geri dönüştürülememenin 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.

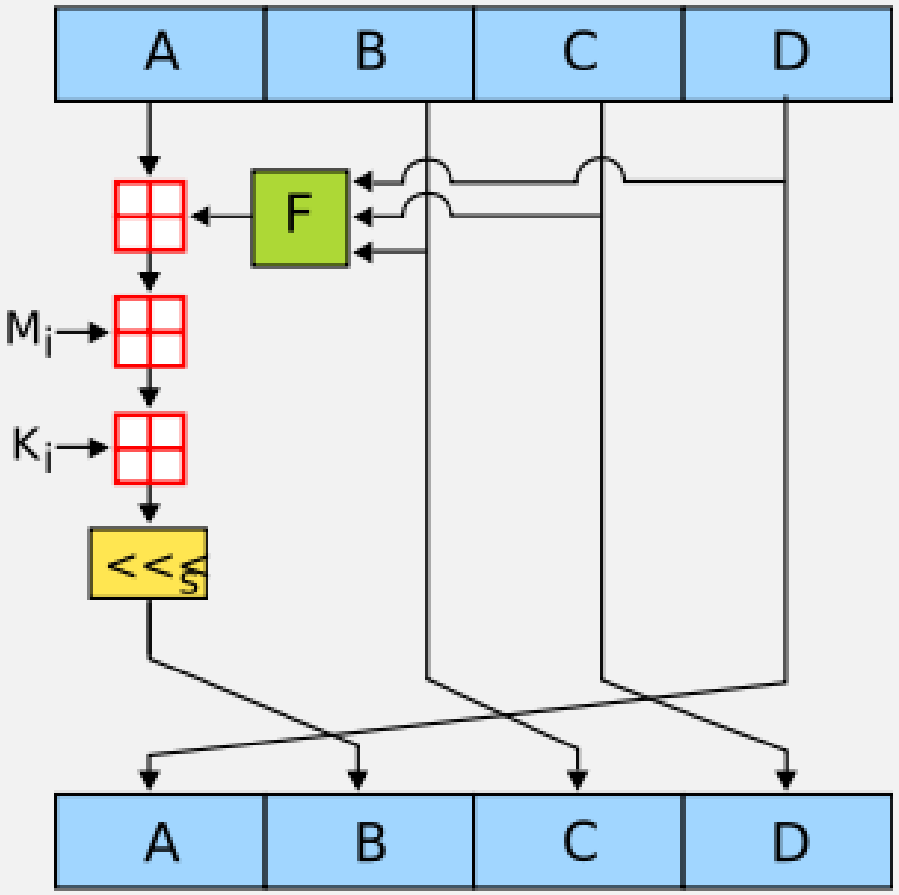
ZAYIFLIĞI

- 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.

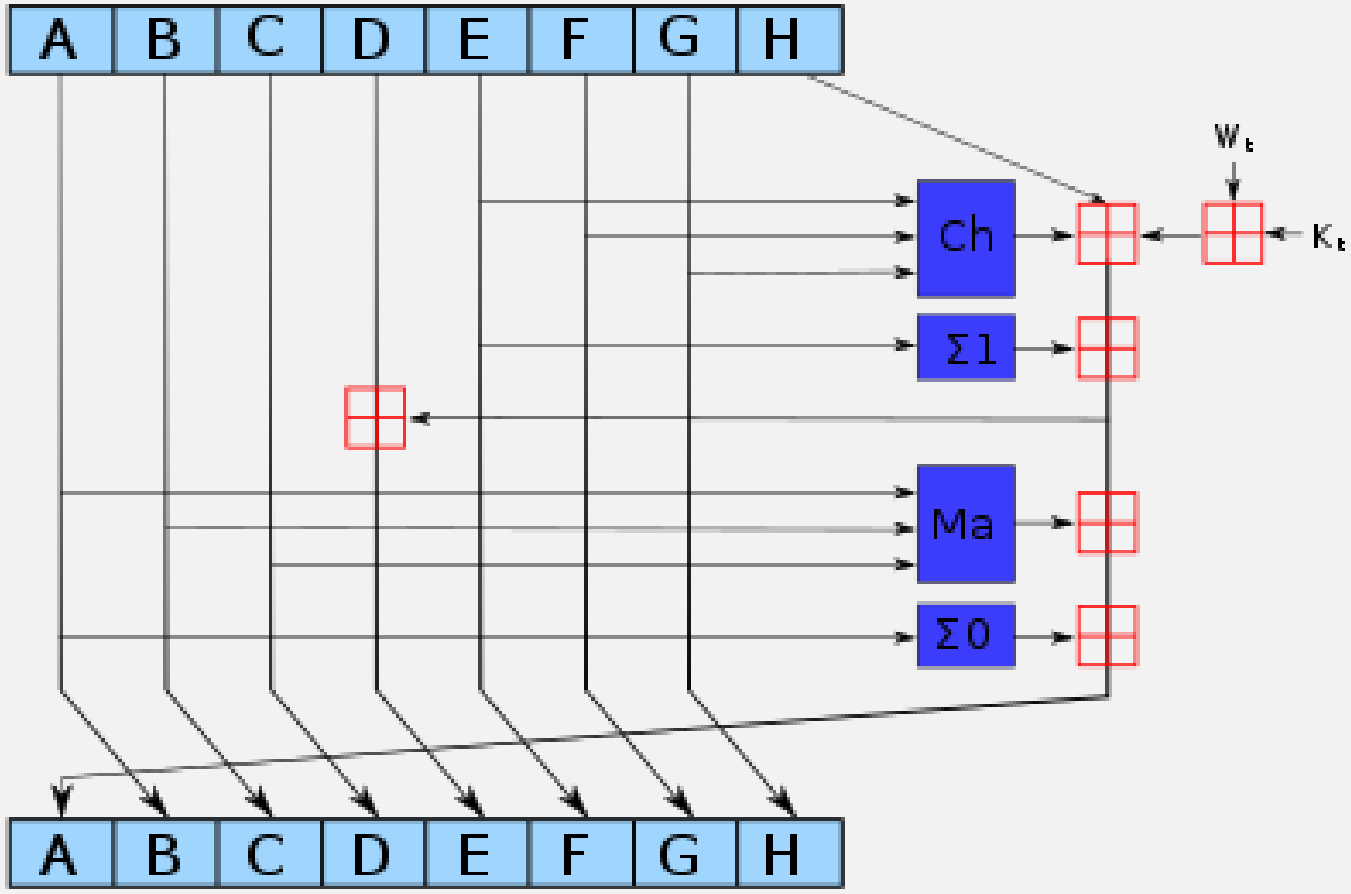
ZAYIFLIK TESTİ

- 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 çekecektiler. Daha sonra ise Google SHA1' e çakışma saldırısı yaptıklarını ve iki farklı PDF dosyasından aynı SHA1 özet çıktıyı aldıklarını ispatlayarak SHA1 in kırıldığını duyurdular.

Algoritma	Özet boyutu (bit)
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