Enigma ve Kriptografi

Mart 2024

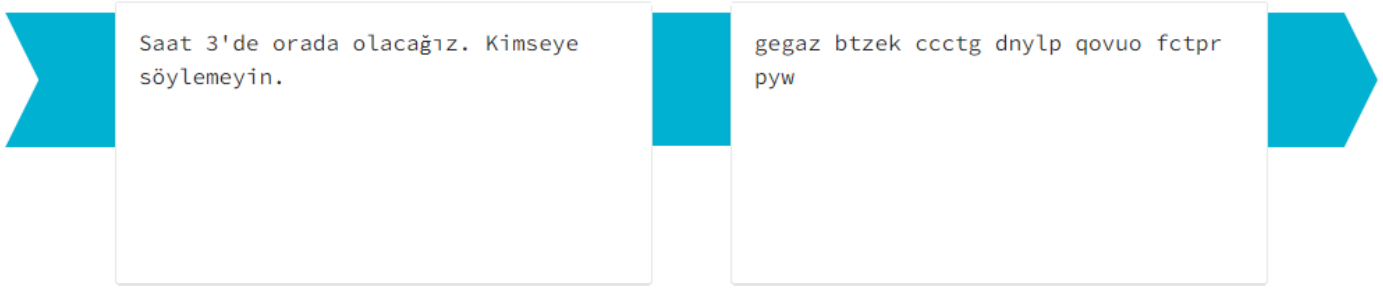
ENIGMA: Model 1 - 1930

Enigma cihazı, ticari, diplomatik ve askeri iletişimi korumak için 20. yüzyılın başlarından ortalarına kadar geliştirilen ve kullanılan bir şifreleme cihazıdır. İkinci Dünya Savaşı sırasında Nazi Almanyası tarafından Alman ordusunun tüm şubelerinde yaygın olarak kullanıldı. Enigma makinesi o kadar güvenli kabul ediliyordu ki, en gizli mesajları şifrelemek için kullanılıyordu.

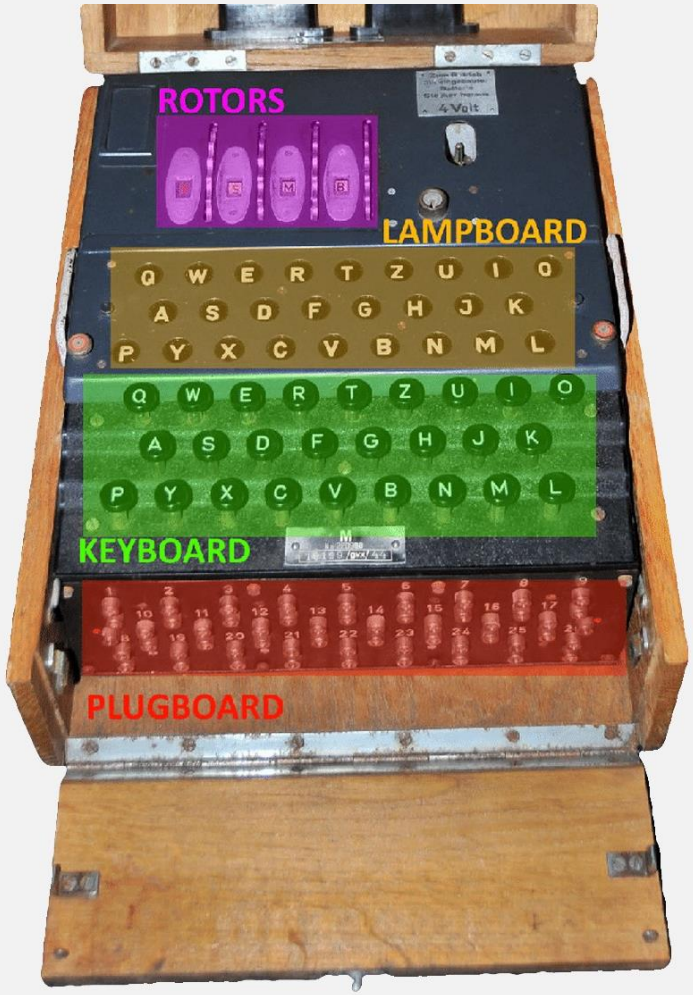
ENIGMA: Şifreleme Temeli

Şifreleme, hassas verileri anlaşılmaz hale getirerek koruma sürecidir. Düz metin, özel bir anahtar veya algoritma kullanılarak şifreli metne dönüştürülür ve sadece şifreyi çözebilecek anahtara sahip kişiler tarafından anlaşılabilir.

Şifreleme, internet üzerinden gönderilen bilgileri ve kişisel verileri korumak için kullanılır. İki ana tipi vardır: **Simetrik şifreleme**, aynı anahtarı şifreleme ve şifre çözme için kullanırken; **asimetrik şifreleme**, farklı bir şifreleme (kamu anahtarı) ve şifre çözme (özel anahtar) anahtarları kullanır.



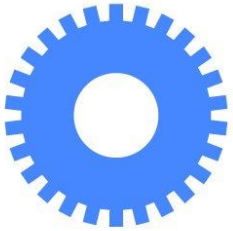
ENIGMA: Çalışma Yapısı 1



Enigma encryption power

5 rotors (choose 3) = 5 x 4 x 3 = **60**

26 rotor starting positions = 26^3 = **17,576**



Plug board choose 10 pairs from 26 letters = $\frac{26!}{6!10!2^{10}}$ = **150,738,274,937,250 (>150 trillion)**

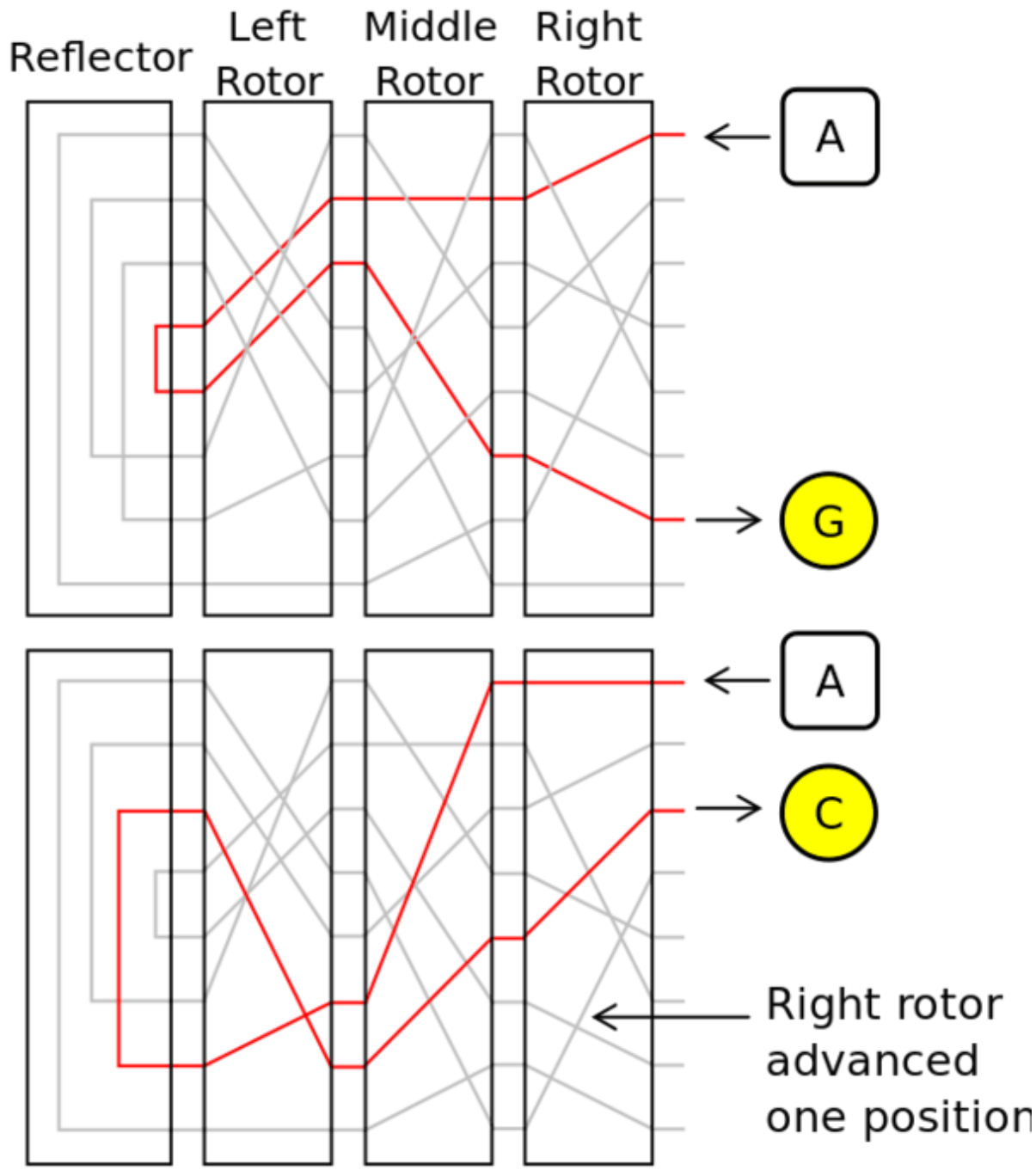
X

= 158,962,555,217,826,360,000 (>158 quintillion)

ENIGMA: Çalışma Yapısı 2

Şifreleme, hassas verileri anlaşılmaz hale getirerek koruma sürecidir. Düz metin, özel bir anahtar veya algoritma kullanılarak şifreli metne dönüştürülür ve sadece şifreyi çözebilecek anahtara sahip kişiler tarafından anlaşılabilir.

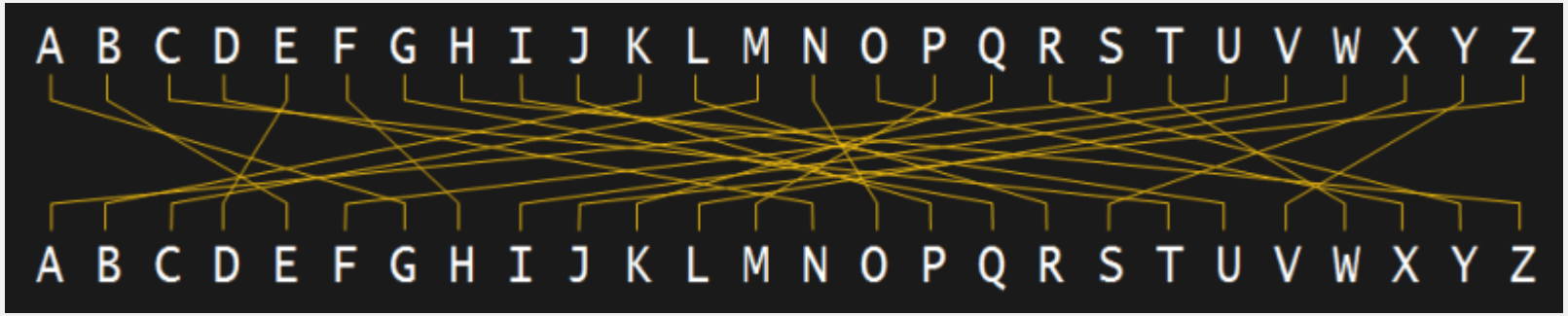
Şifreleme, internet üzerinden gönderilen bilgileri ve kişisel verileri korumak için kullanılır. İki ana tipi vardır: **Simetrik şifreleme**, aynı anahtarı şifreleme ve şifre çözme için kullanırken; **asimetrik şifreleme**, farklı bir şifreleme (kamu anahtarı) ve şifre çözme (özel anahtar) anahtarları kullanır.

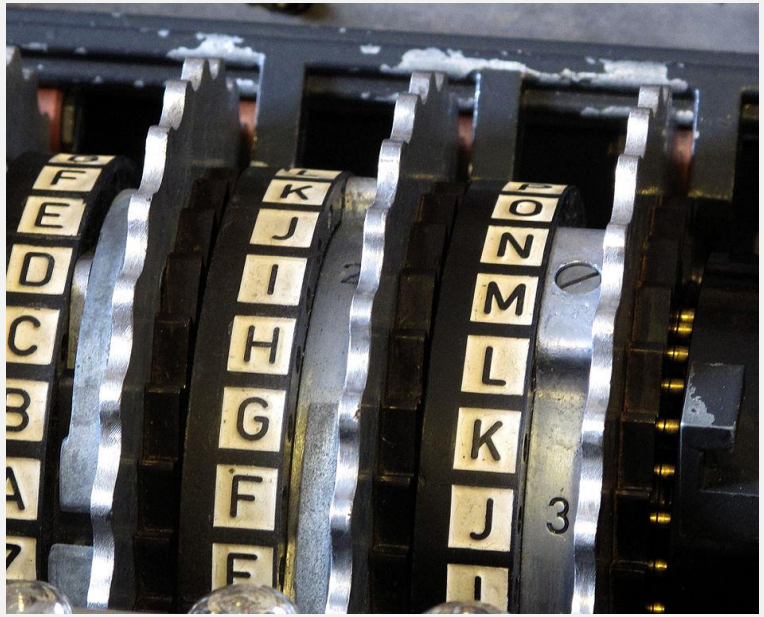


ENIGMA: Çalışma Yapısı 3

SIMPLE SUBSTITUTION CIPHER

ADDING ROTORS





ROTORS

$i#r3l3m3

Kriptografi: Gizemin Şifresi

Kriptografi, bilgileri güvenli bir şekilde saklama ve iletimini sağlayan bir bilim ve sanat dalıdır. Kelime anlamı olarak Yunanca 'gizli yazı' anlamına gelen "kryptós" (gizli) ve "graphein" (yazmak) kelimelerinden türetilmiştir.

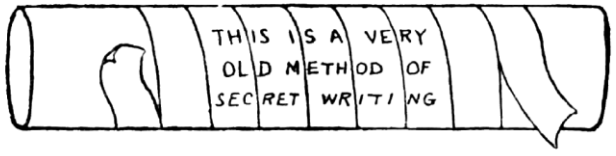
Tarihi Kökenleri

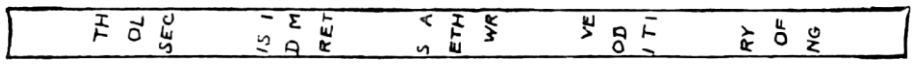
Kriptografinin kökenleri, insanlık tarihi kadar eskiye dayanır. İlk şifreleme yöntemleri, M.Ö. 1900 yıllarında Antik Mısır'da hiyerogliflerin kullanılmasıyla ortaya çıktı.

Kriptografi: Scytale

Kriptografi sanatının en eski bilinen örneklerinden biri, M.Ö. 5. yüzyılda Yunanistan'da kullanılan Scytale adlı bir şifreleme aracıdır.

Scytale ilkel bir yer değiştirme şifrelemesidir.

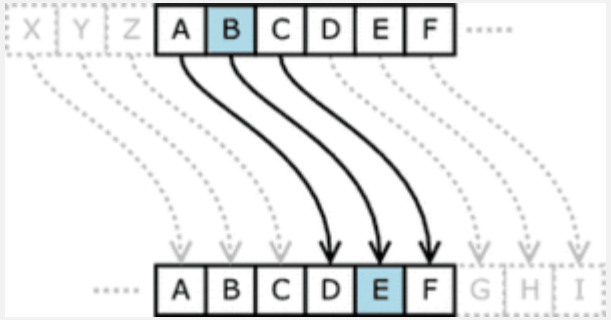


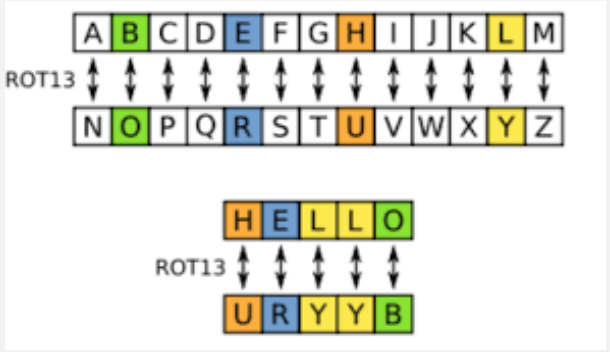


Kriptografi: Sezar Şifrelemesi

Latin alfabesindeki harflerin yer değiştirmesi ile oluşturulan bu yöntemde kullanılan her harf aslında kendisinden sonraki üçüncü harfi işaret eder.

A harfi D harfini temsil eder. Z harfi ise C.





Hashing vs Encryption

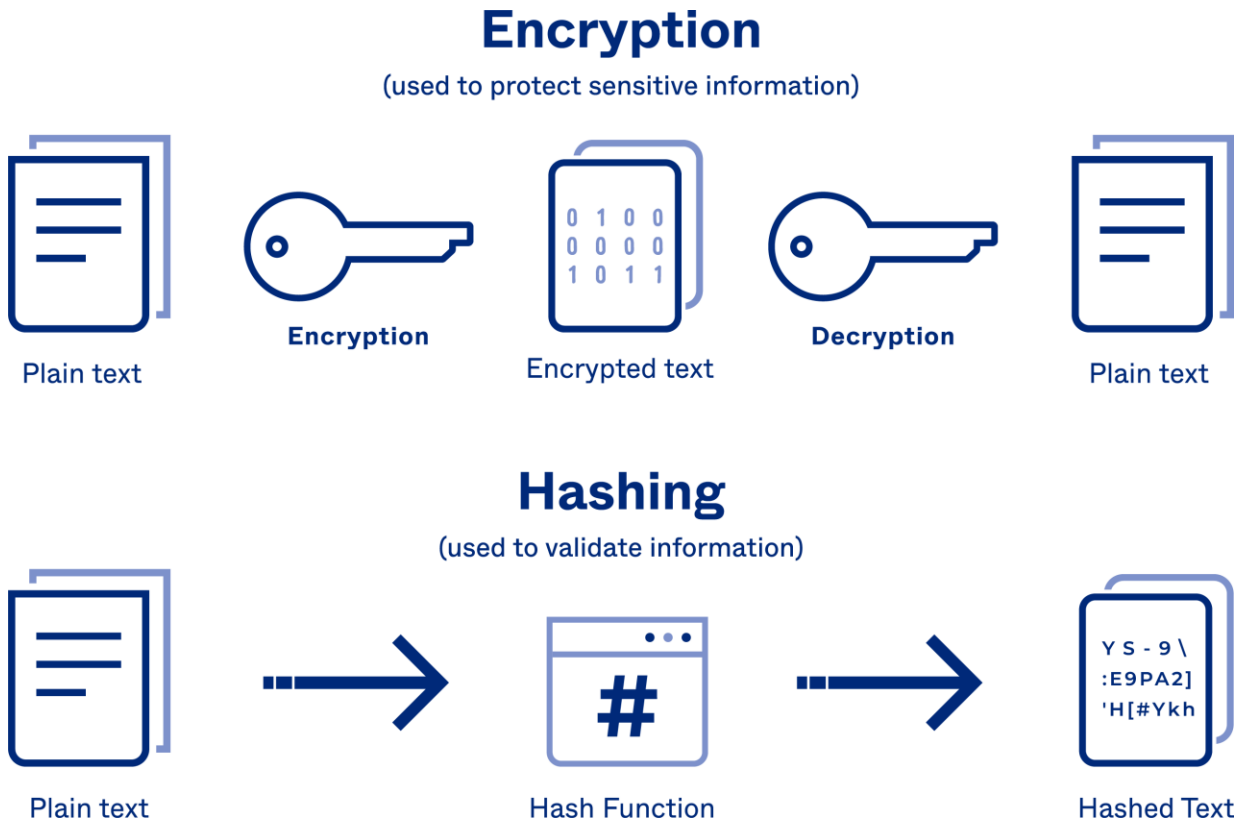
Bazı insanlar şifreleme ve karma terimlerini eş zamanlı olarak kullanır. Gerçekten de her ikisi de bilgileri korumak için kullanılır, ancak çok farklı yollarla yaparlar.

Encryption (Şifreleme)

Bir anahtarla çözülebilen verileri karıştırır. Amaç, bilgiyi başka bir tarafa aktarmaktır ve alıcı, verileri deşifre etmek için anahtarları kullanacaktır.

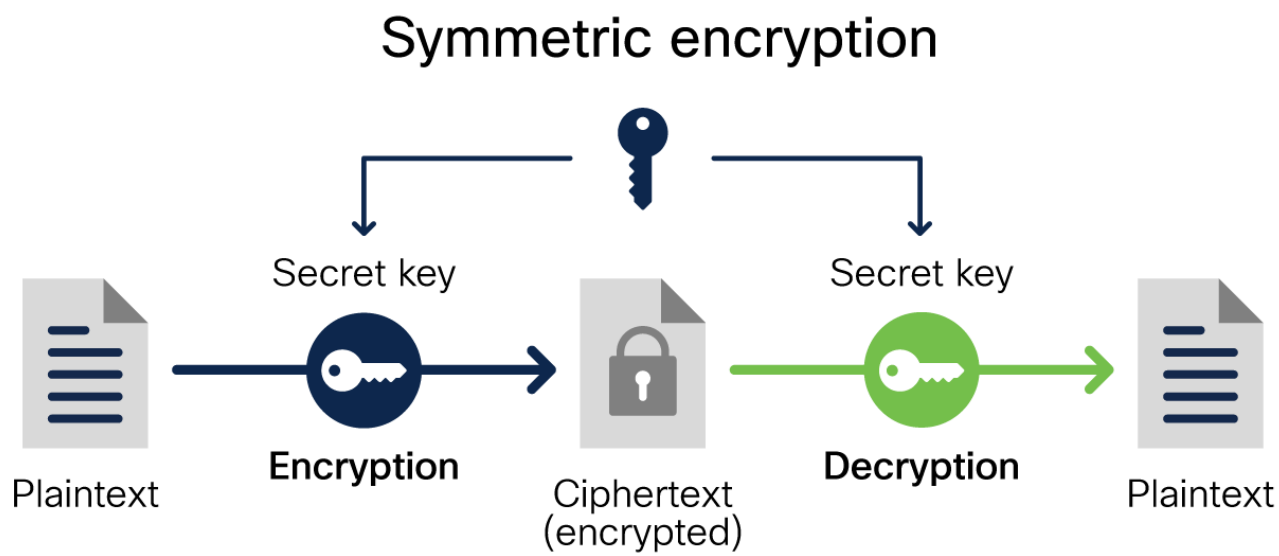
Hash (Karma)

Karma da verileri karıştırır, ancak amaç otantikliğini kanıtlamaktır. Çözümleme anahtarı yoktur.



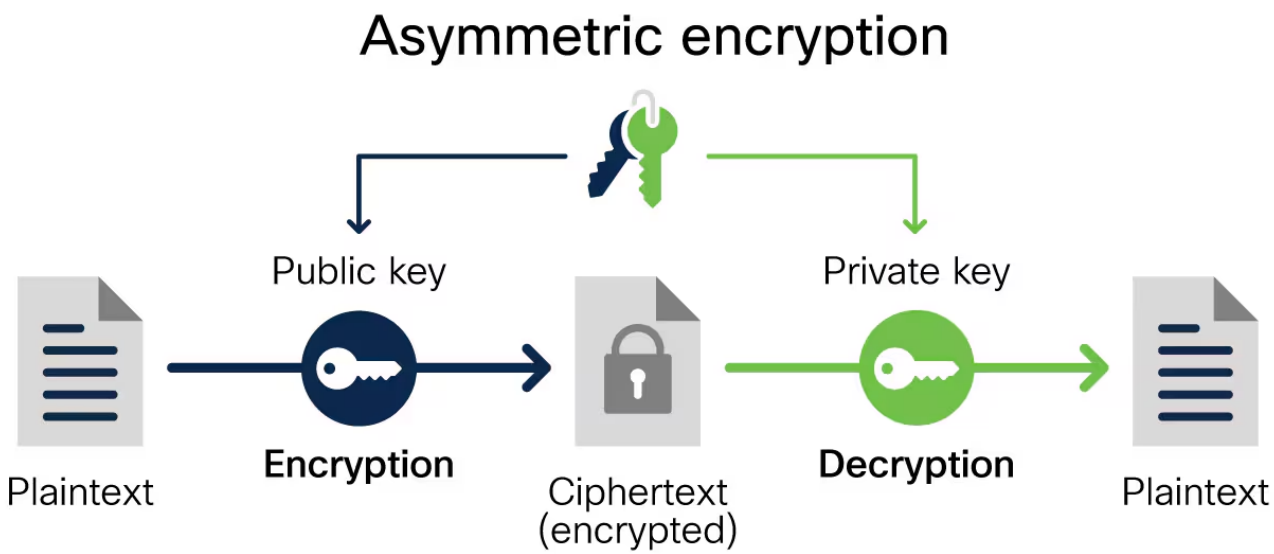
Symmetric Encryption

Simetrik şifreleme, şifreleme ve şifre çözme için aynı anahtarı kullanır. Aynı anahtarı kullandığı için, simetrik şifreleme, sağladığı güvenlik açısından daha maliyet etkin olabilir. Bununla birlikte, simetrik şifreleme kullanılırken verilerin güvenli bir şekilde saklanmasına daha fazla yatırım yapmak önemlidir.



Asymmetric Encryption

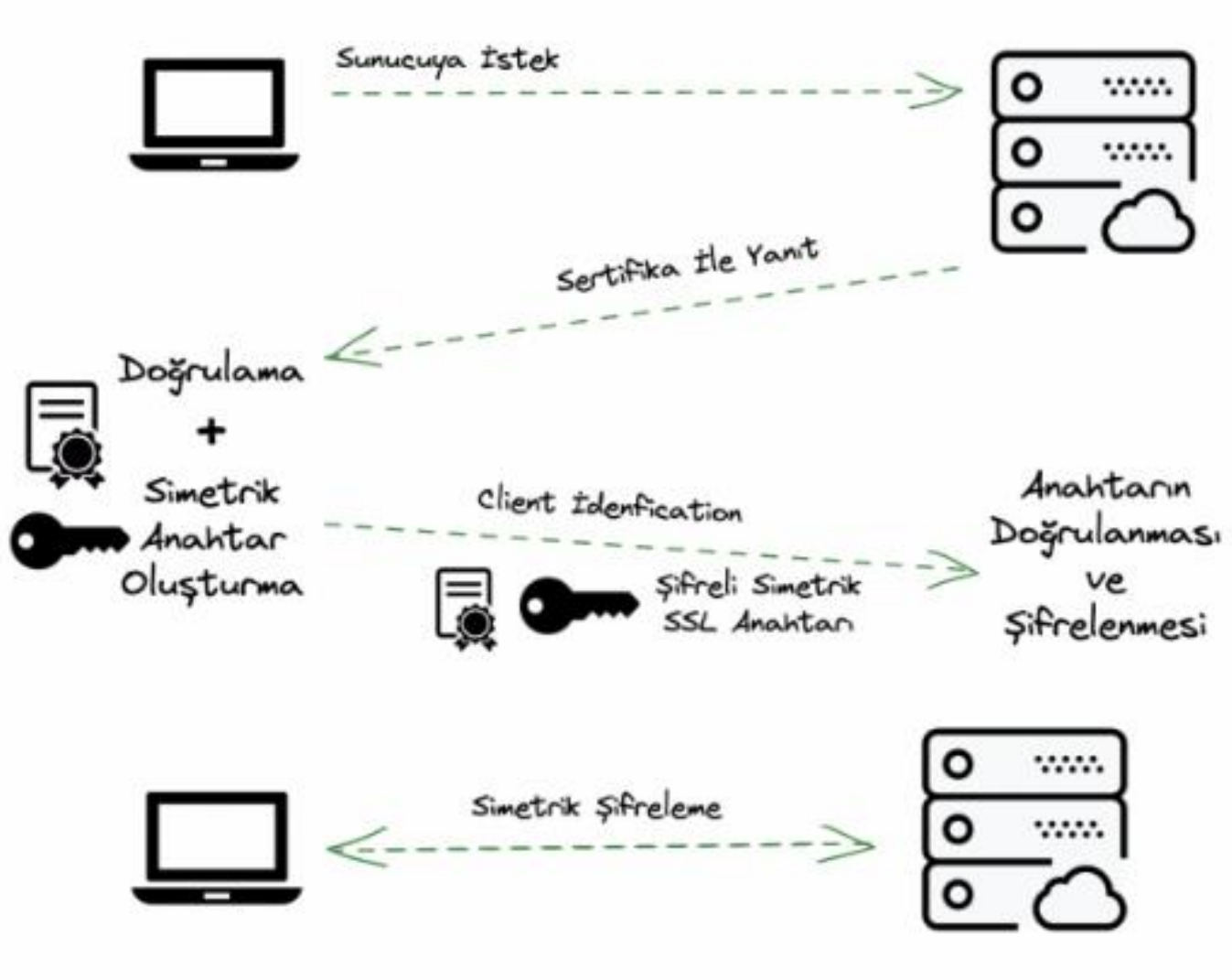
Asimetrik şifreleme, iki ayrı anahtar kullanır: bir kamu anahtarı ve bir özel anahtar. Genellikle verileri şifrelemek için kamu anahtarı kullanılırken, verilerin şifresini çözmek için özel anahtar gereklidir. Özel anahtar sadece yetkili erişime sahip kullanıcılara verilir. Sonuç olarak, asimetrik şifreleme daha etkili olabilir, ancak maliyeti de daha yüksektir.



SSL - TLS

TLS (Transport Layer Security) ve **SSL (Secure Sockets Layer)**, internet üzerinden güvenli veri iletişimini sağlayan kriptografik protokollerdir. SSL, 1990'ların ortalarında geliştirilen ilk protokolken, TLS, SSL'in daha gelişmiş ve güvenli bir versiyonudur.

Her iki protokol de, web tarayıcıları ve sunucular arasındaki veri aktarımını şifreleyerek, hassas bilgilerin yetkisiz erişime karşı korunmasına yardımcı olur. HTTPS protokolü bu güvenliği sağlamak için genellikle TLS kullanır. Kısacası, TLS ve SSL, internet üzerindeki güvenli iletişimin temelini oluşturur.



Kaynaklar

Enigma Machine
https://en.wikipedia.org/wiki/Enigma_machine

Enigma Emulator
https://www.101computing.net/enigma-machine-emulator/

Enigma Encryptor
https://cryptii.com/pipes/enigma-machine

TLS
https://en.wikipedia.org/wiki/Transport_Layer_Security

Encryption
https://en.wikipedia.org/wiki/Encryption

TEŞEKKÜRLER

ekinokssoftware.com

ekinokssoftware