ALİCE, BOB and OSCAR

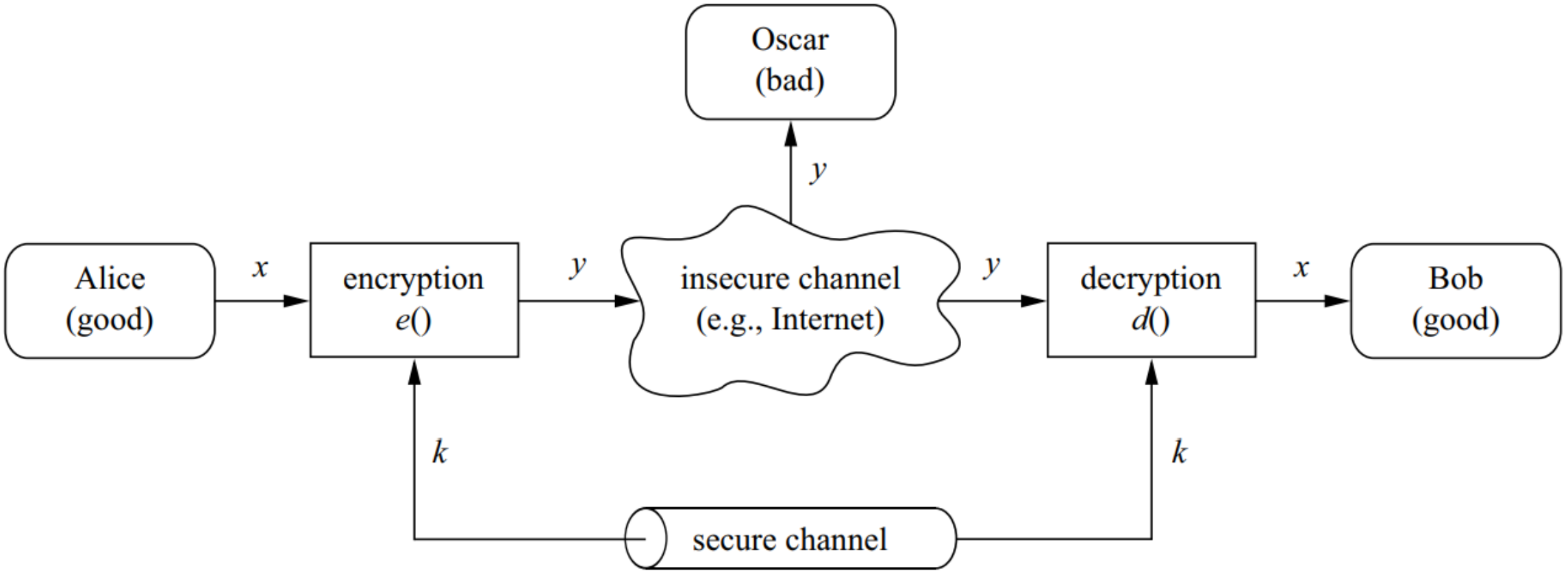
In cryptography, Alice and Bob are fictional characters commonly used as placeholders in cryptographic protocols or systems, discussions and other science and engineering literature with several participants in a thought experiment.

Oscar is the 3rd person to listen to messages between Bob and Alice.

Kriptografide, Alice ve Bob, kriptografik protokollerde veya sistemlerde, birkaç katılımcının bulunduğu tartışmalarda ve diğer bilim ve mühendislik literatürlerinde bir düşünce deneyinde yer tutucu olarak yaygın bir şekilde kullanılan kurgusal karakterlerdir.

Oscar, Bob ve Alice arasındaki mesajları dinleyen üçüncü kişidir.

ALİCE, BOB and OSCAR



Symmetric Algorithms

Symmetric Algorithms are what many people assume cryptography is about: two parties have an encryption and decryption method for which they share a secret key. All cryptography from ancient times until 1976 was exclusively based on symmetric methods. Symmetric ciphers are still in widespread use, especially for data encryption and integrity check of messages.

Simetrik Algoritmalar, birçok insanın kriptografinin aşağıdakilerle ilgili olduğunu varsaydığı şeydir: iki tarafın, gizli bir anahtarı paylaştıkları bir şifreleme ve şifre çözme yöntemi vardır. Antik çağlardan 1976'ya kadar olan tüm kriptografi tamamen simetrik yöntemlere dayanıyordu. Simetrik şifreler, özellikle veri şifreleme ve mesajların bütünlük kontrolü için hala yaygın olarak kullanılmaktadır.

Asymmetric Algorithms

Asymmetric (or Public-Key) Algorithms in 1976 an entirely different type of cipher was introduced by Whitfield Diffie, Martin Hellman and Ralph Merkle. In public-key cryptography, a user possesses a secret key as in symmetric cryptography but also a public key. Asymmetric algorithms can be used for applications such as digital signatures and key establishment, and also for classical data encryption.

Asimetrik (veya Açık Anahtarlı) Algoritmalar 1976'da Whitfield Diffie, Martin Hellman ve Ralph Merkle tarafından tamamen farklı bir şifre türü olarak tanıtıldı. Açık anahtarlı kriptografide, kullanıcı simetrik şifrelemede olduğu gibi gizli bir anahtara ve aynı zamanda bir açık anahtara sahiptir. Asimetrik algoritmalar, dijital imzalar ve anahtar oluşturma gibi uygulamalarda ve ayrıca klasik veri şifrelemede kullanılabilir.

Cryptographic Protocols

- **Cryptographic Protocols** Roughly speaking, crypto protocols deal with the application of cryptographic algorithms. Symmetric and asymmetric algorithms can be viewed as building blocks with which applications such as secure Internet communication can be realized. The Transport Layer Security (TLS) scheme, which is used in every Web browser, is an example of a cryptographic protocol.
- **Kriptografik Protokoller** kabaca konuşursak, kripto protokolleri kriptografik algoritmaların uygulanmasıyla ilgilenir. Simetrik ve asimetrik algoritmalar, güvenli İnternet iletişimi gibi uygulamaların gerçekleştirilebileceği yapı taşları olarak görülebilir. Her Web tarayıcısında kullanılan Taşıma Katmanı Güvenliği (TLS) şeması, bir kriptografik protokol örneğidir.

Stream Ciphers

Stream Ciphers

If we look at the types of cryptographic algorithms that exist in a little bit more detail, we see that the symmetric ciphers can be divided into stream ciphers and block ciphers, as shown in Fig. 2.1.

Var olan kriptografik algoritma türlerine biraz daha detaylı bakarsak, simetrik şifrelerin Şekil 2.1'de gösterildiği gibi akış şifreleri (stream cipher) ve blok şifrelerine (block cipher) bölünebileceğini görürüz.

Encryption Methods

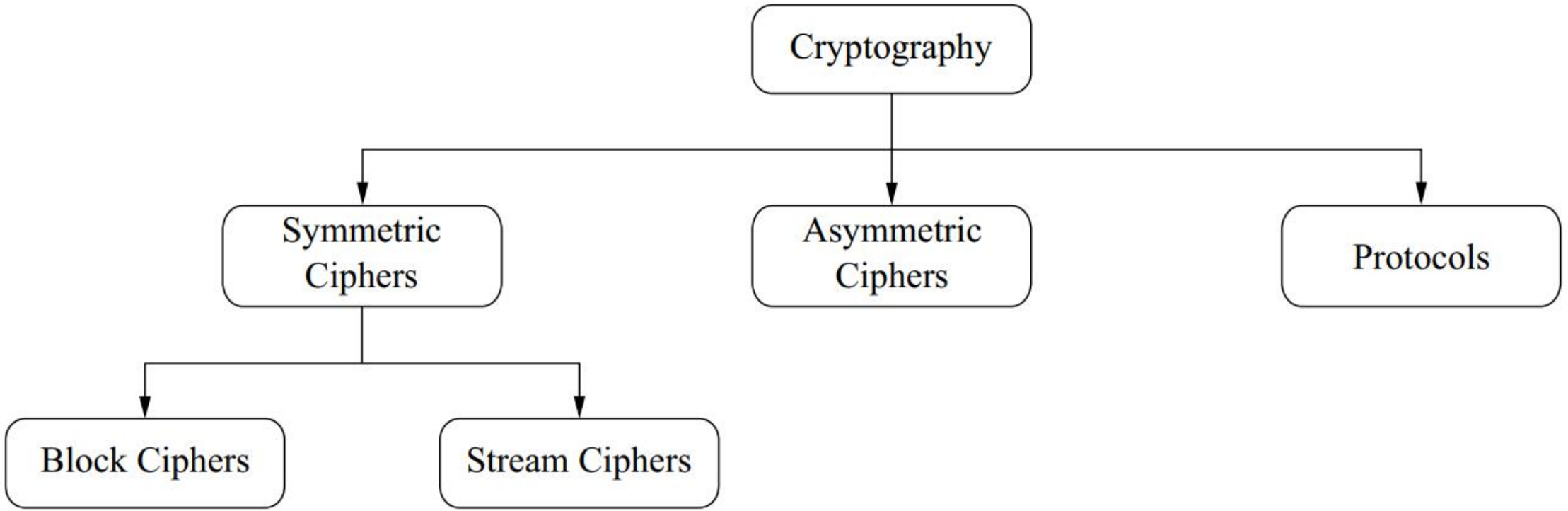


Fig. 2.1 Main areas within cryptography

Stream Cipher

Stream ciphers encrypt bits individually. This is achieved by adding a bit from a key stream to a plaintext bit. There are synchronous stream ciphers where the key stream depends only on the key, and asynchronous ones where the key stream also depends on the ciphertext.

Akış şifreleri, bitleri ayrı ayrı şifreler. Bu, bir anahtar akışından bir düz metin bitine bir bit eklenerek elde edilir. Anahtar akışının yalnızca anahtara bağlı olduğu eşzamanlı akış şifreleri ve anahtar akışının da şifreli metne bağlı olduğu eşzamansız şifreler vardır.

Stream Ciphers

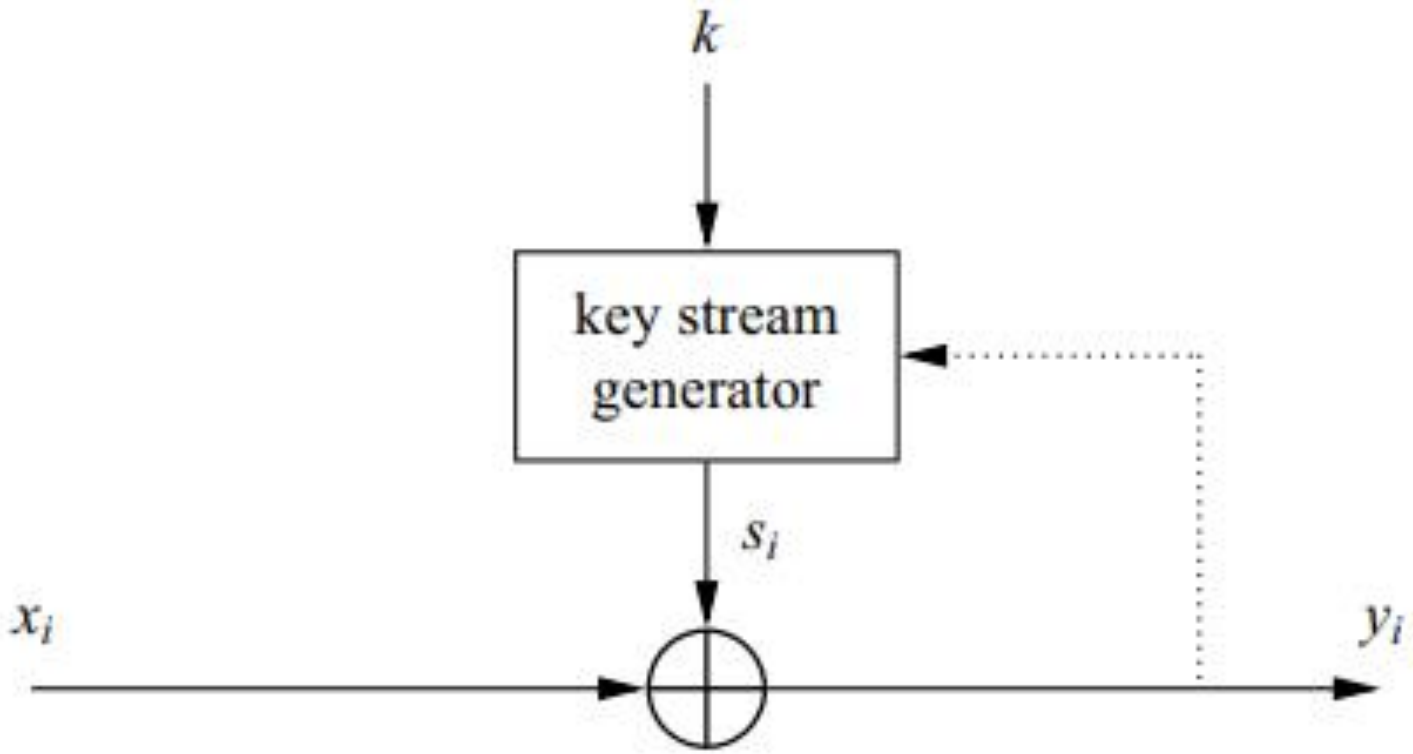


Fig. 2.3 Synchronous and asynchronous stream ciphers

Block Ciphers

Block ciphers encrypt an entire block of plaintext bits at a time with the same key. This means that the encryption of any plaintext bit in a given block depends on every other plaintext bit in the same block. In practice, the vast majority of block ciphers either have a block length of 128 bits (16 bytes) such as the advance encryption standard (AES), or a block length of 64 bits (8 bytes) such as the data encryption standard (DES) or triple DES (3DES) algorithm.

Blok şifreleri, aynı anahtarla aynı anda tüm düz metin bitleri bloğunu şifreler. Bu, belirli bir bloktaki herhangi bir düz metin bitinin şifrelenmesinin, aynı bloktaki diğer tüm düz metin bitlerine bağlı olduğu anlamına gelir. Pratikte, blok şifrelerin büyük çoğunluğu, ileri şifreleme standardı (AES) gibi 128 bitlik (16 bayt) blok uzunluğuna veya veri şifreleme standardı (DES) ya da üçlü DES (3DES) algoritması gibi 64 bitlik (8 bayt) blok uzunluğuna sahiptir.)

The Data Encryption Standard (DES) and Alternatives

Introduction to DES

→Data Encryption Standard (DES) encrypts blocks of size 64 bit.

→Developed by IBM based on the cipher Lucifer under influence of the National Security Agency (NSA), the design criteria for DES have not been published.

→Veri Şifreleme Standardı (DES) 64 bitlik blokları şifreler.

→Ulusal Güvenlik Ajansı'nın (NSA) etkisi altında Lucifier şifresine dayalı olarak IBM tarafından geliştirilen DES için tasarım kriterleri yayınlanmamıştır.

The Data Encryption Standard (DES) and Alternatives

→ Most Popular block cipher for most of the last 30 years.

→ By far best studied symmetric algorithm.

→ Nowadays considered insecure due to the small key length of 56 bit.

→ Son 30 yılın en popüler blok şifresi.

→ Şimdiye kadar en iyi çalışılmış simetrik algoritmadır.

→56 bitlik küçük anahtar uzunluğu nedeniyle günümüzde güvensiz kabul edilmektedir.

The Advanced Encryption Standard (AES)

AES is the most widely used symmetric cipher today.

The algorithm for AES was chosen by the US National Unstitute of Standards and Technology (NIST) in a multi-year selection process.

AES, günümüzde en yaygın kullanılan simetrik şifredir.

AES algoritması, ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından uzun yıllar süren bir seçim sürecinde seçilmiştir.

The Advanced Encryption Standard (AES)

The requirements for all AES candidate submission were:

1. Block cipher with 128-bit block size
2. Three supportd key lengths: 128, 192 and 256 bit

AES algoritmasının aday olmasında etkili olan tüm gereksinimleri şunlardı:

1. 128 bitlik blok boyutlu blok şifresi
2. Desteklenen üç anahtar uzunluğu: 128, 192 ve 256 bit.

The Advanced Encryption Standard (AES)

The requirements for all AES candidate submission were:

3- Security relative to other submitted algorithms

4- Efficiency in software and hardware

AES algoritmasının aday olmasında etkili olan tüm gereksinimleri şunlardı:

3- Gönderilen diğer algoritmalara göre güvenli olması.

4- Yazılım ve donanımda verimlilik.

The Advanced Encryption Standard (AES)

- **Overview of the AES Algorithm**
- The AES cipher is almost identical to the block cipher Rijndael. The Rijndael block and key size vary between 128, 192 and 256 bits. However, the AES standard only calls for a block size of 128 bits. Hence, only Rijndael with a block length of 128 bits is known as the AES algorithm.

- AES şifresi, blok şifresi Rijndael ile neredeyse aynıdır. Rijndael bloğu ve anahtar boyutu 128, 192 ve 256 bit arasında değişir. Ancak, AES standardı yalnızca 128 bitlik bir blok boyutu gerektirir. Bu nedenle, yalnızca 128 bitlik blok uzunluğuna sahip Rijndael, AES algoritması olarak bilinir.