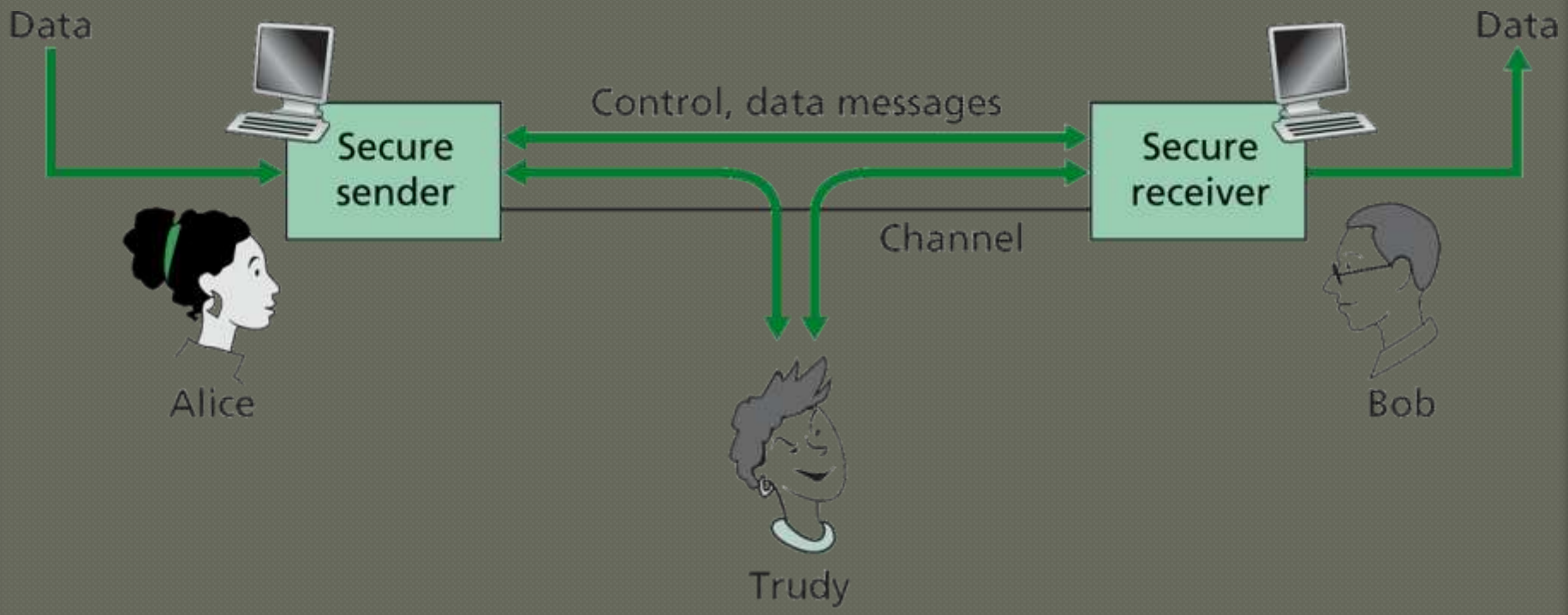
Сетевые информационные технологии

Курс лекций

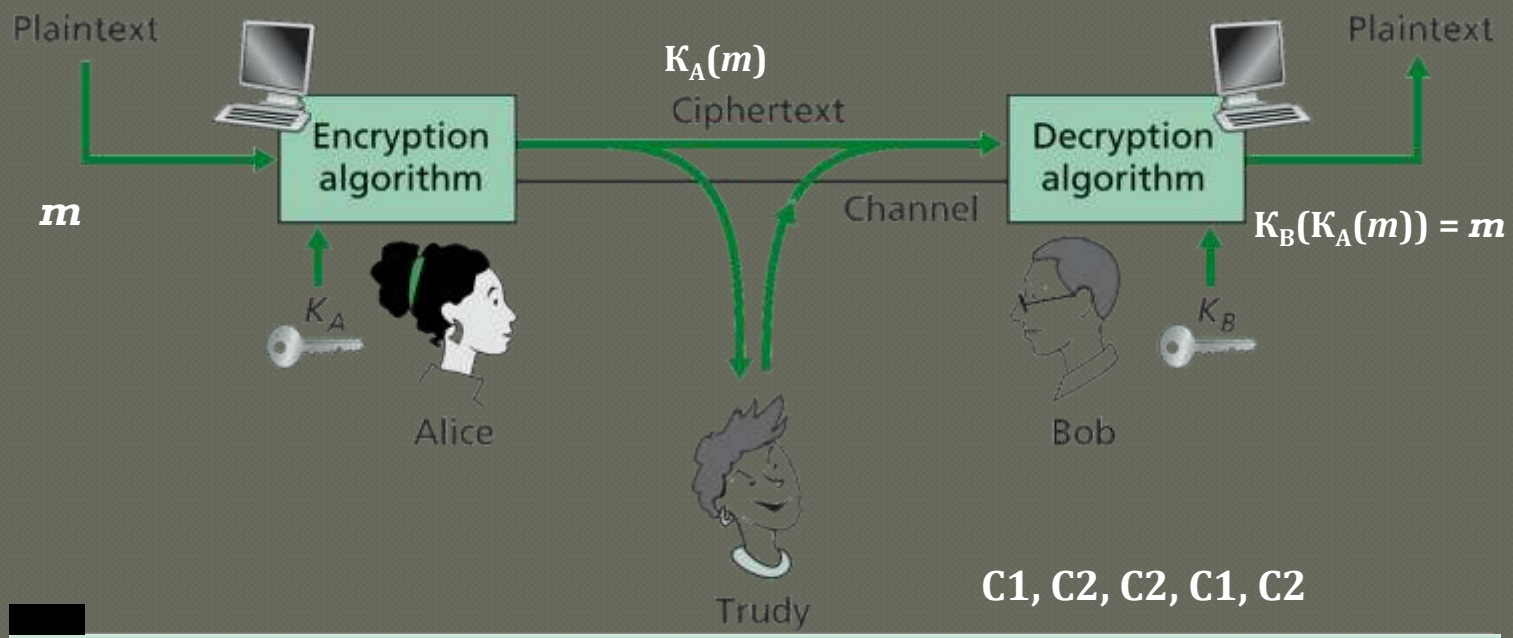
Лекция 12

Сетевая безопасность



- Конфиденциальность
- Аутентификация
- Целостность сообщения
- Управление доступом

Шифрование

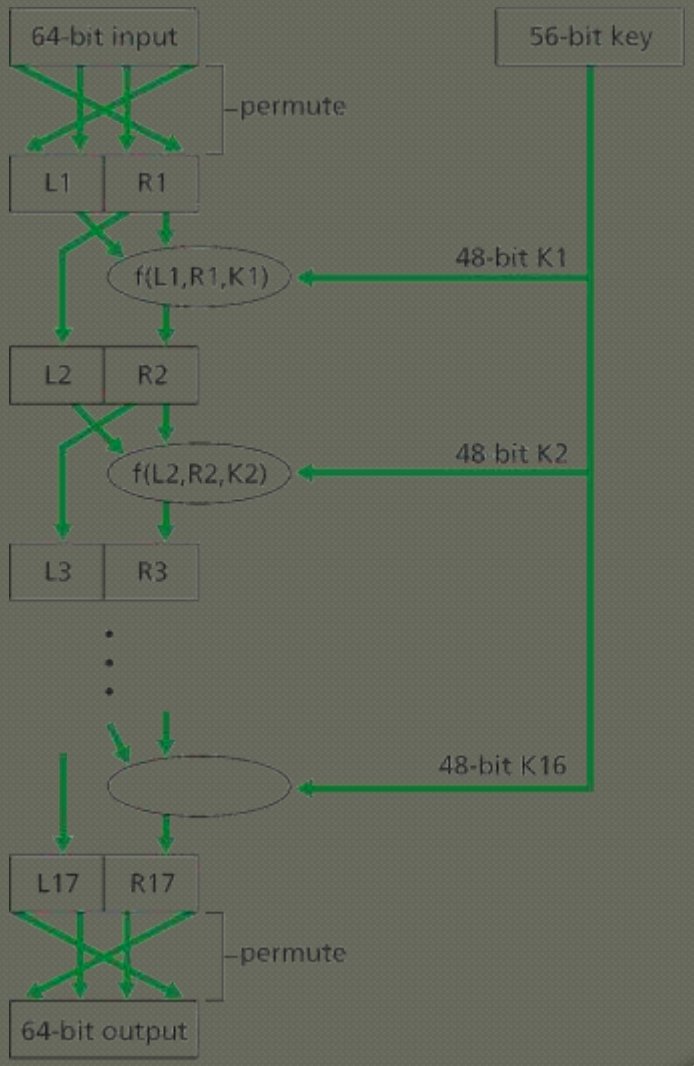


C1, C2, C2, C1, C2

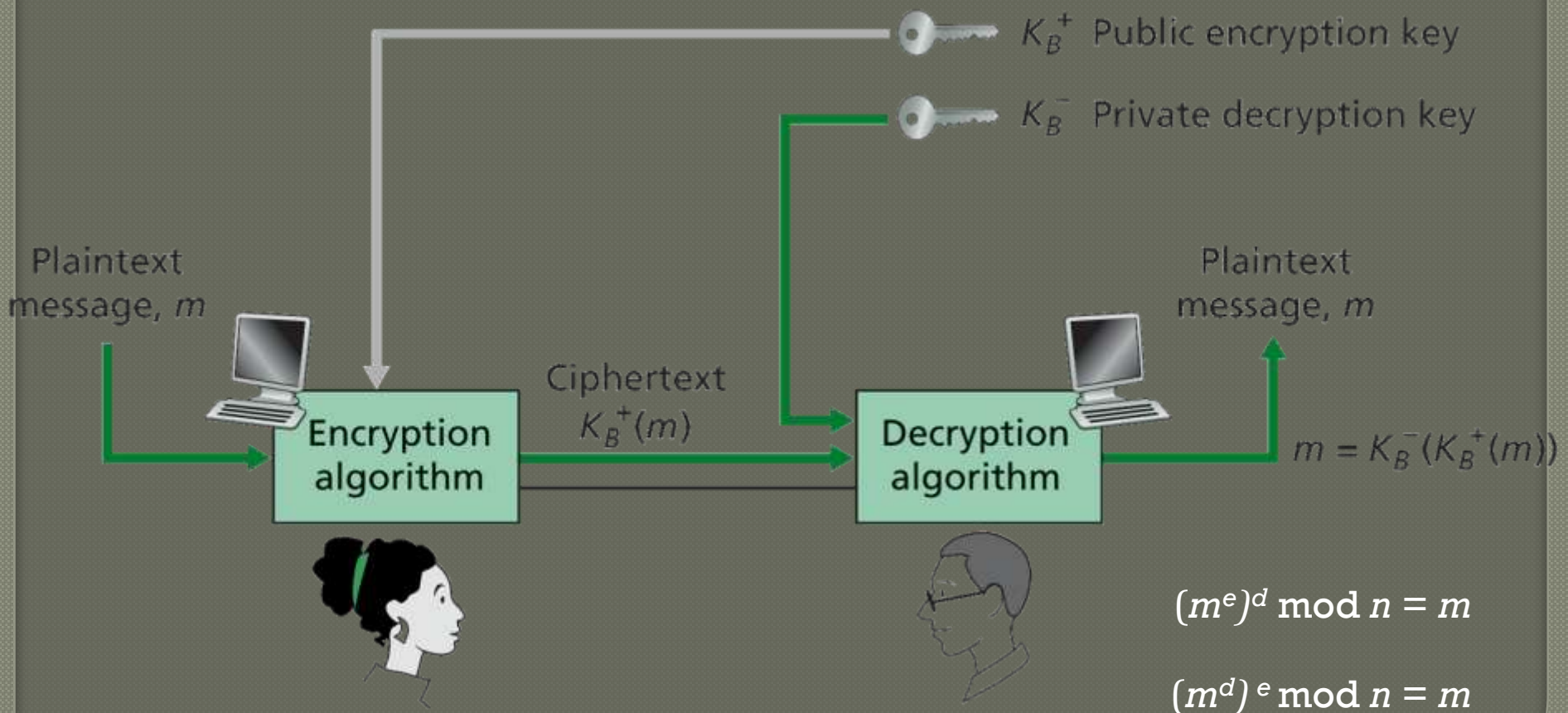
Plaintext letter:	a b c d e f g h i j k l m n o p q r s t u v w x y z
$C_1(k = 5)$:	f g h i j k l m n o p q r s t u v w x y z a b c d e
$C_2(k = 19)$:	t u v w x y z a b c d e f g h i j k l m n o p q r s

Алгоритм DES

- шифр DES кодирует 64-разрядные блоки кода при помощи 64-разрядного ключа
- шифр AES (Advanced Encryption Standard) кодирует данные 128-разрядными блоками при помощи ключей длиной 128, 192 и 256 бит



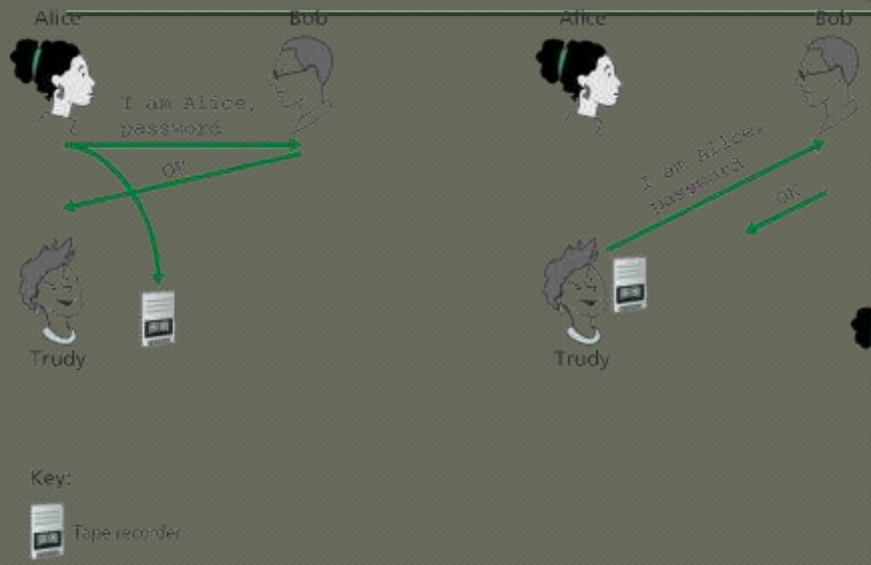
Шифрование открытым ключом



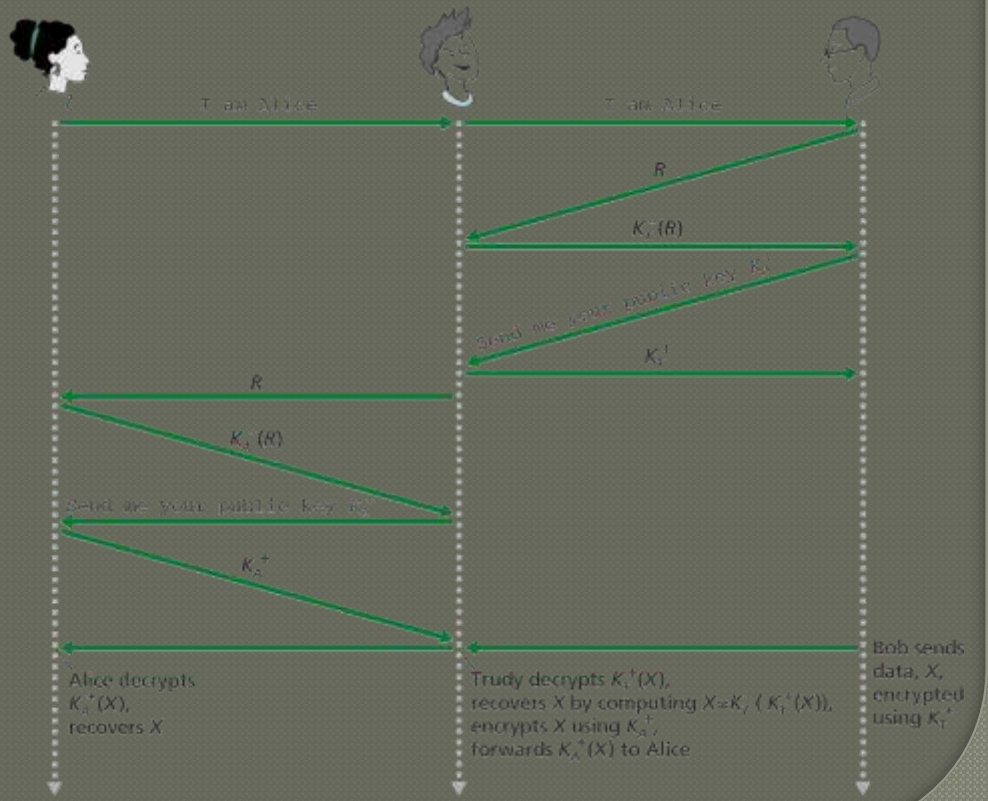
$(m^e)^d \bmod n = m$

$(m^d)^e \bmod n = m$

Аутентификация

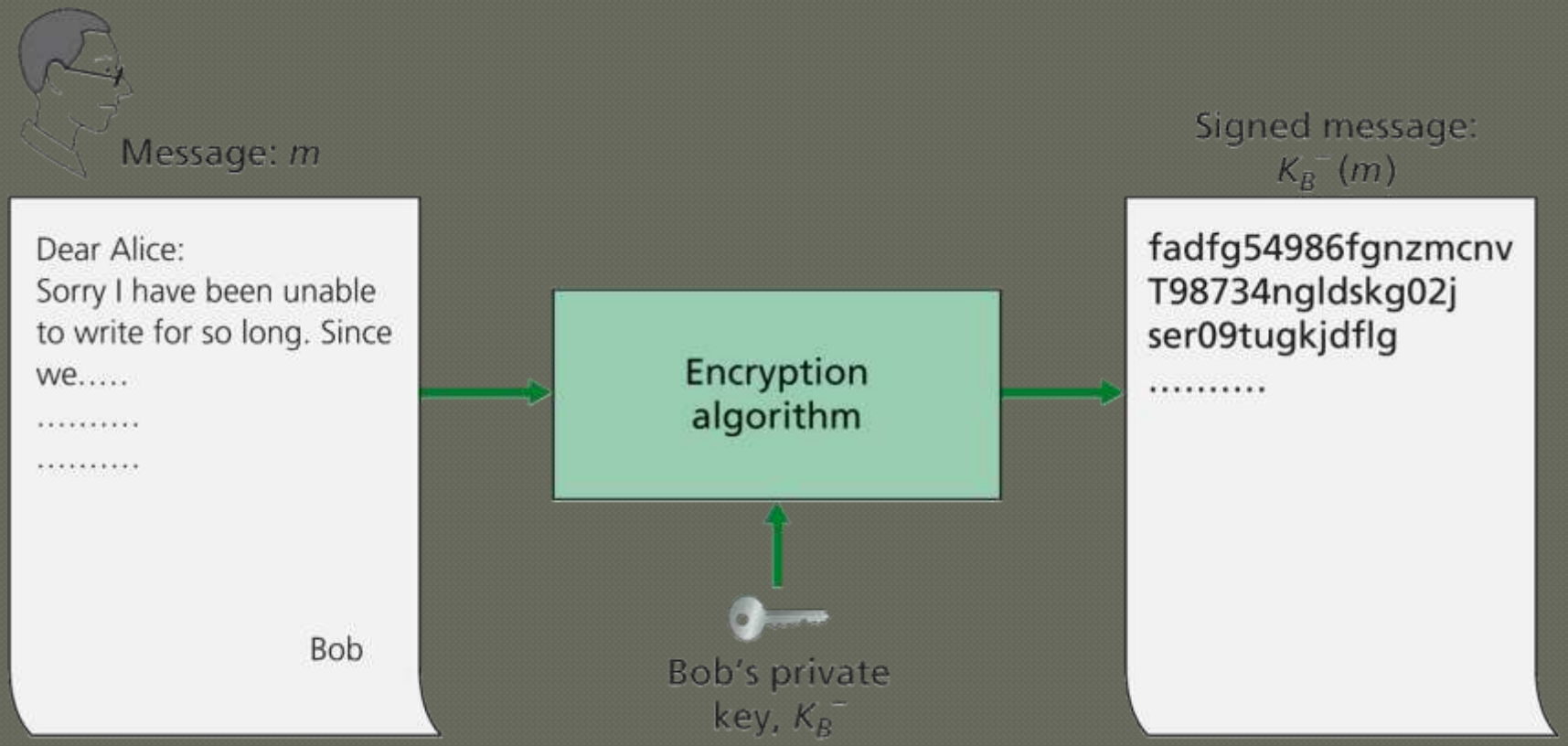


Аутентификацией называют процесс подтверждения чьей-либо личности

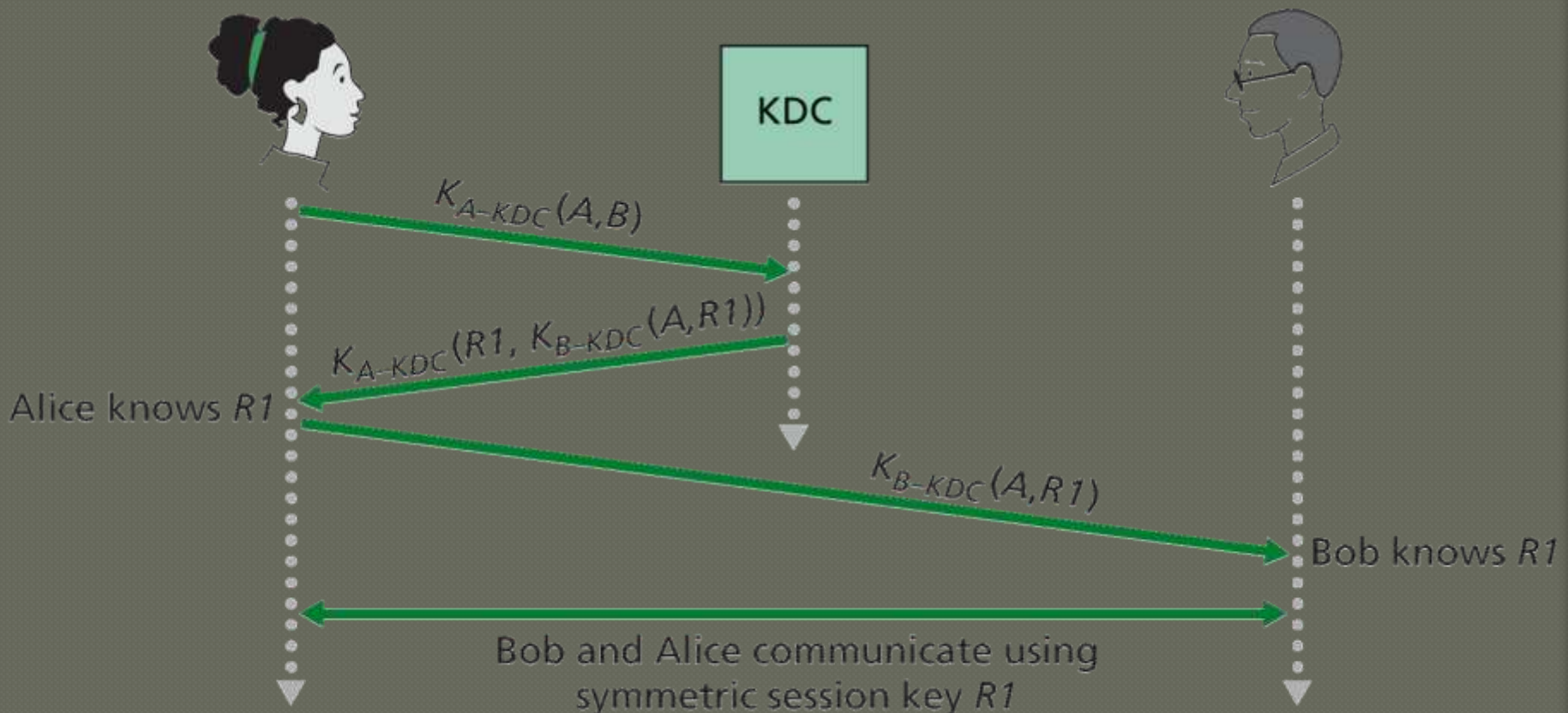


Цифровая подпись должна быть выполнена таким образом, чтобы ее невозможно было подделать и чтобы от нее невозможно было отречься

Цифровая подпись

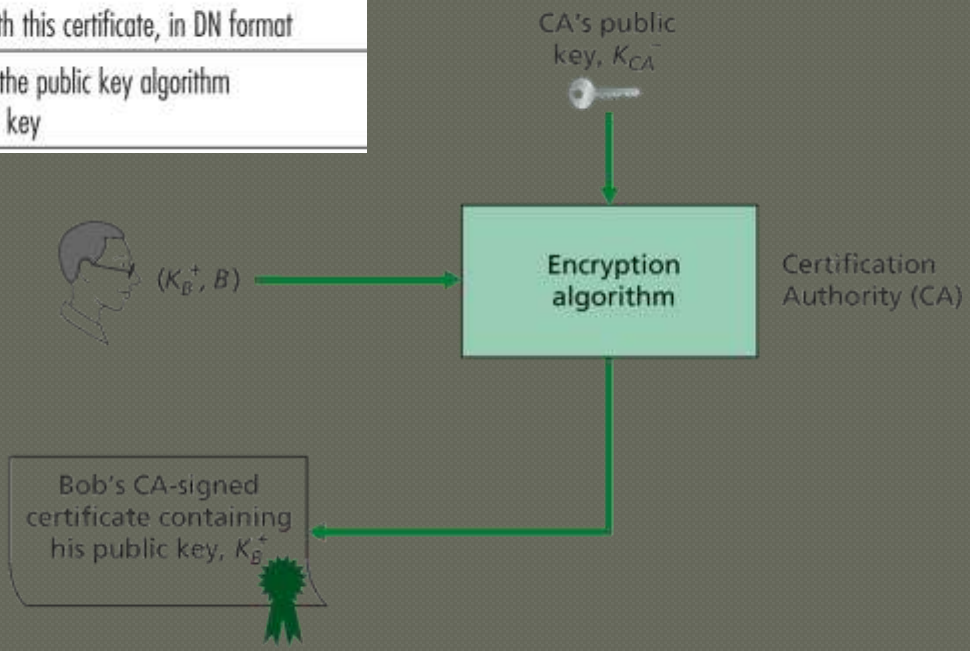


Key Distribution Center



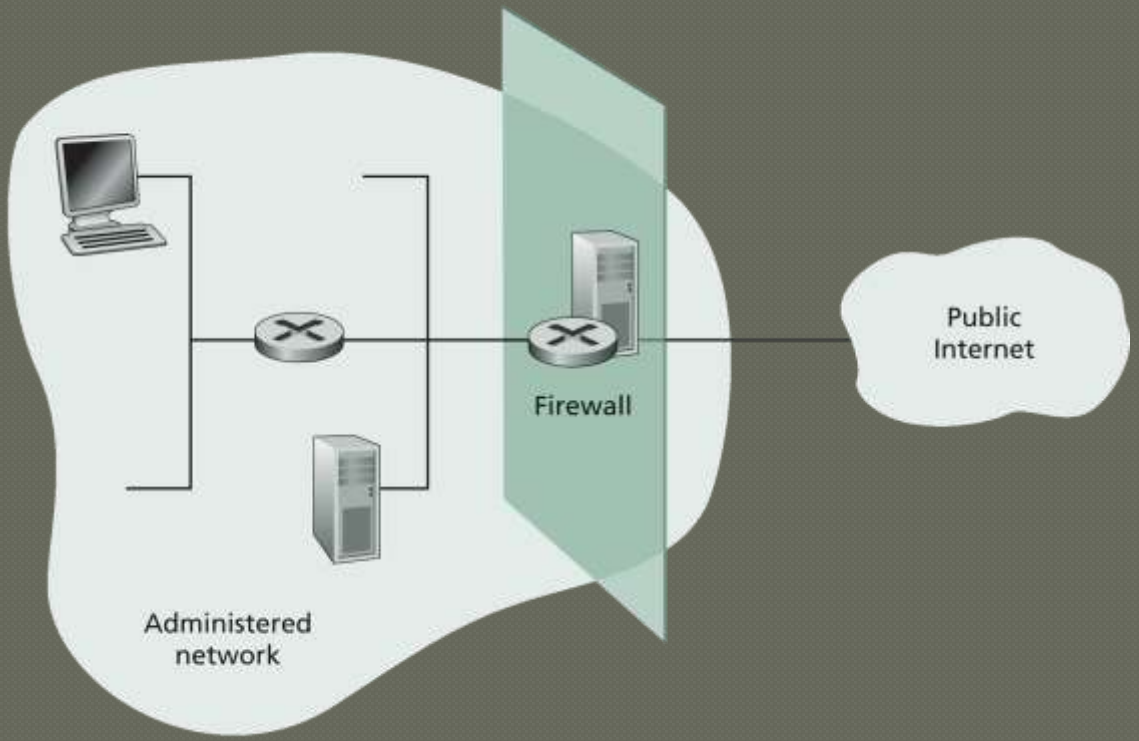
Сертификация

Field Name	Description
Version	Version number of X.509 specification
Serial Number	CA-issued unique identifier for a certificate
Signature	Specifies the algorithm used by CA to sign this certificate
Issuer Name	Identity of CA issuing this certificate, in distinguished name (DN) [RFC 2253] format
Validity period	Start and end of period of validity for certificate
Subject name	Identity of entity whose public key is associated with this certificate, in DN format
Subject public key	The subject's public key as well as an indication of the public key algorithm (and algorithm parameters) to be used with this key



Брандмауэр

- проверяет входящий и исходящий трафик
  - *брандмауэры, фильтрующие пакеты*
  - *шлюзы прикладного уровня*



Цикл лекций подготовлен в 2010 году Кузнецовым Игорем Ростиславовичем, доцентом кафедры радиоэлектронных средств Санкт-Петербургского государственного электротехнического университета им. В. И. Ульянова (Ленина)

Прочитан в дисциплине
«Сетевые информационные технологии»