Криптография в .NET

Кондратьев Денис
Visual .NET User Group
vng.visualdesign.ru

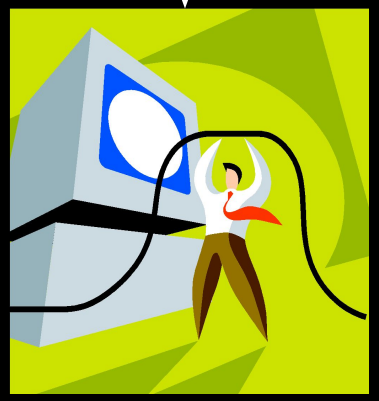
Криптография в .NET

- Основы криптографии
- Введение в криптографические алгоритмы
- Пространство имен Cryptography
- Примеры кода
- Q&A

Alice и Bob

Alice

Bob



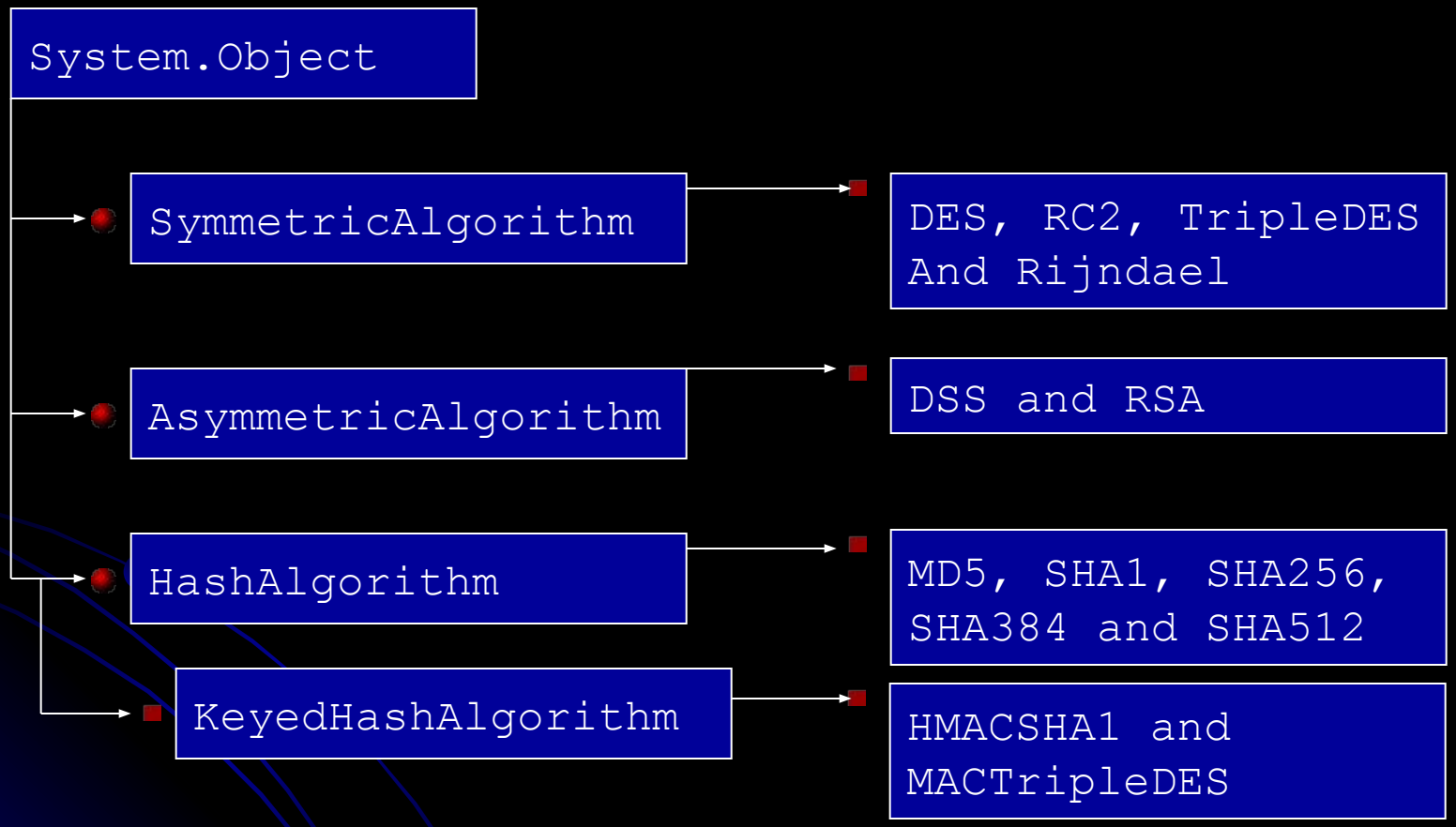
Задачи криптографии

- **Конфиденциальность:** защита данных от просмотра
- **Целостность данных:** защита от изменений
- **Аутентификация:** подтверждение источника данных

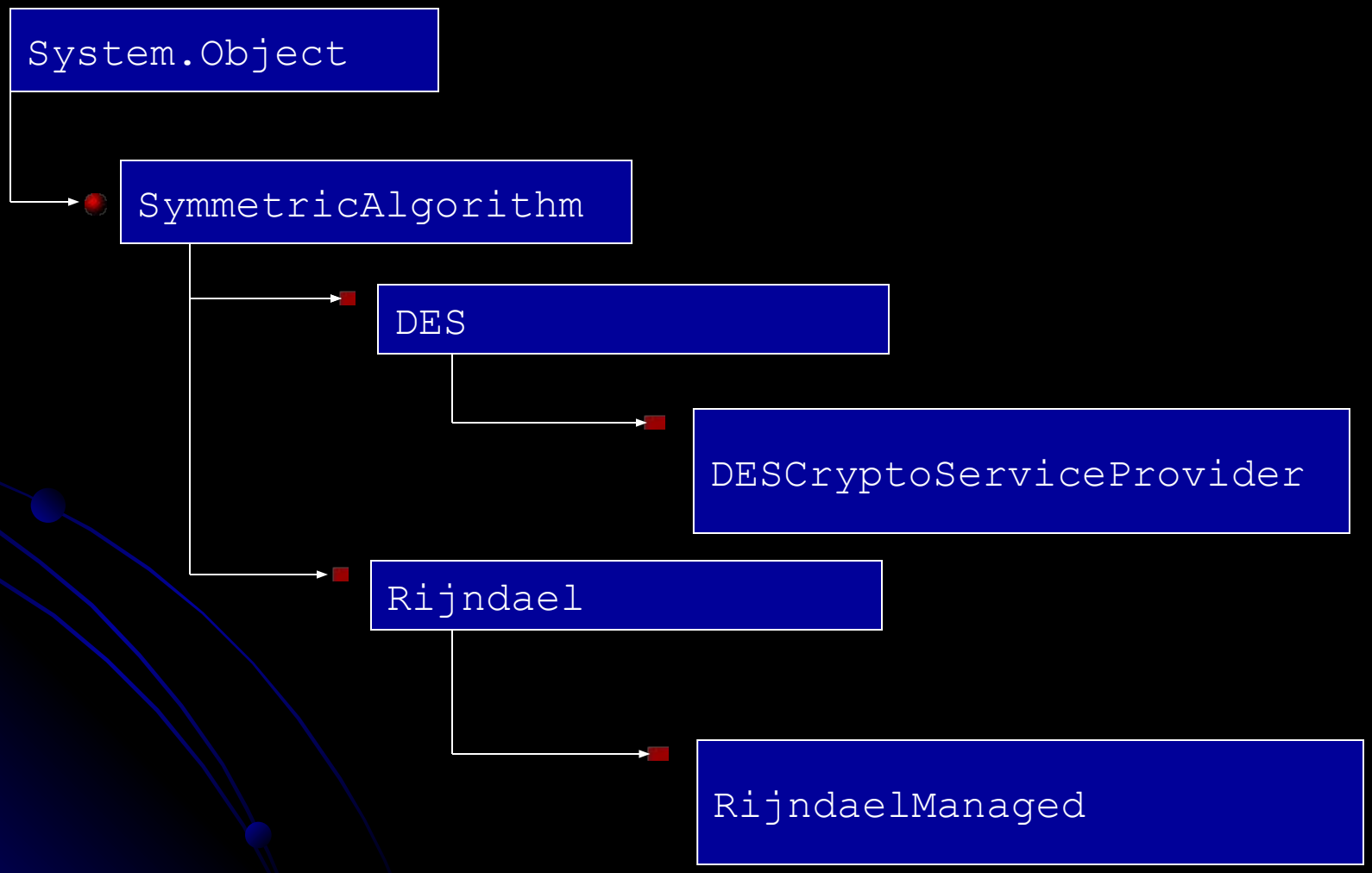
Криптографические алгоритмы

- симметричные алгоритмы
- ассиметричные алгоритмы
- алгоритмы для получения хеша данных
- алгоритмы для подписи данных

System.Security.Cryptography



Структура классов



Симметричные алгоритмы

Alice (закрыть

акрытый ключ)

E(M,K)

C,K)= M

- .NET реализация
  - DES
  - Triple-DES
  - RC2
  - Rinjdael

M = сообщение
E = шифрование
D = дешифрование
C = зашифрованный текст

Длина ключа

Алгоритм	Возможный размер ключа	Размер ключа по умолчанию
DES	64 bit	64 bit
RC2	40 to 128 bit	128 bit
Triple-DES	128, 192 bit	192 bit
Rijndael	128, 192, 256 bit	256 bit

Классы .NET

- DESCryptoServiceProvider
- RC2CryptoServiceProvider
- RijndaelManaged
- TripleDESCryptoServiceProvider

Использование симметричных алгоритмов

Имя	Описание
Key	Ключ
KeySize	Размер ключа в битах
LegalKeySizes	Возможные размеры ключей
IV	Инициализирующий вектор
CreateEncryptor()	Создает объект с интерфейсом ICryptoTransform на основе ключа и IV для шифрования данных
CreateDecryptor()	Создает объект с интерфейсом ICryptoTransform на основе ключа и IV для дешифровки данных
GenerateKey()	Создает случайный ключ
GenerateIV()	Создает случайный ключ

Пример кода

DES

Шифрование с открытым ключом

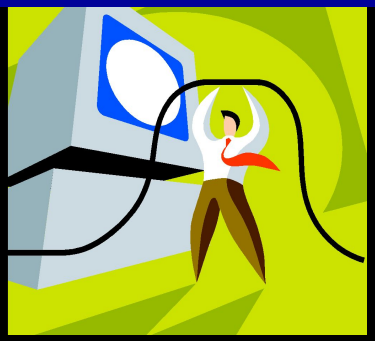
Alice (открытый

закрытый ключ)

E(M,K)

C,K)= M

- .NET реализация
  - DSS (Digital Signature Standard)
  - RSA



M = сообщение
E = шифрование
D = дешифрование
C = зашифрованный текст

Классы .NET

- DSACryptoServiceProvider
- RSACryptoServiceProvider

Шифрование с открытым ключем

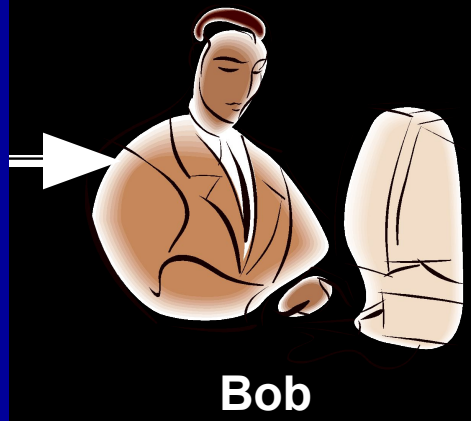
Члены класса	Описание
KeySize	Размер ключа в битах
FromXmlString()	Создает объект, инкапсулирующий алгоритм, из XML данных
ToXmlString()	Возвращает XML представление объекта, инкапсулирующего алгоритм

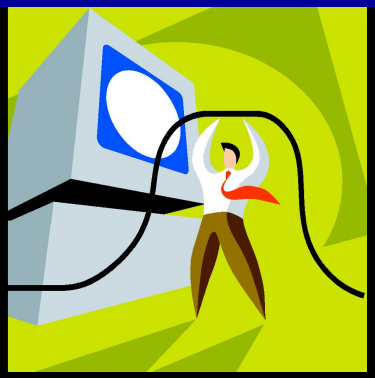
Пример кода

RSA

Хеширование

- .NET реализация
  - MD5
  - SHA1
  - SHA256
  - SHA384
  - SHA512





Классы .NET

- HMACSHA1
- MACTripleDES
- MD5CryptoServiceProvider
- SHA1Managed
- SHA256Managed
- SHA384Managed
- SHA512Managed

Хеширование

Член класса	Описание
ComputeHash()	Расчитывает хеш на основе массива байт или потока
HashSize Hash	Размер хеша в битах
Hash	Возвращает расчитанный хеш

Пример кода

MD5

Цифровая подпись

- SignatureDescription
- DSACryptoServiceProvider
- RSACryptoServiceProvider

SignData

- public byte[] SignData(byte[] *buffer*);
- public byte[] SignData(byte[] *buffer*, int *offset*, int *count*);
- public byte[] SignData(Stream *inputStream*);

SignHash

- public byte[] SignHash(byte[] rgbHash() , string str)

Пример кода

DSA

Q&A