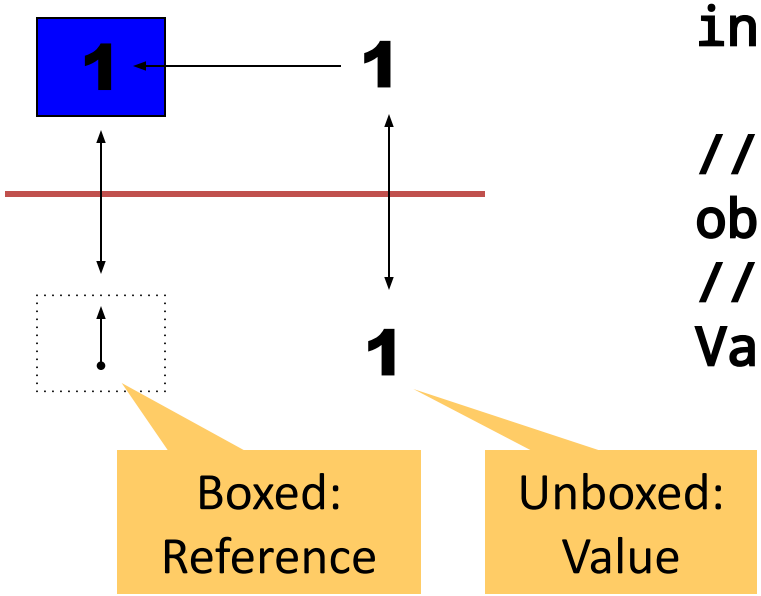
ЛЕКЦИЯ №13

Москва, 2019

Boxing и Unboxing

- Типы-значения могут быть преобразованы к объекту (boxed) и обратно (unboxed)
- Boxing – преобразование значения в объект
- Основано на объектном представлении любого типа
- Boxing обычно выполняется неявно, в отличие от Java (“классов-оберток”)
- Boxing / unboxing *не является CLS-совместимой операцией*
- Java 1.5: Sun решил ввести boxing и unboxing в Java (наряду с классами-обертками)




```
int Value;

// Boxing
object BoxedValue = Value;
// Unboxing
Value = (int)BoxedValue;
```

Net Security Framework

- AES AES (Advanced Encryption Standard) - это симметричный алгоритм. Он был разработан для обоих
- программное и аппаратное обеспечение. Он поддерживает 128-битные данные и 128,192,256-битный ключ.
- DES DES (Стандарт шифрования данных) - симметричный алгоритм, опубликованный Национальным институтом
- стандарта и технологии (NIST).
- RC2 RC2 (код Рона или шифр Ривеста), также известный как ARC2, представляет собой симметричный алгоритм, разработанный Рон Ривест.
- Rijndael Rijndael - это симметричный алгоритм, выбранный АНБ в качестве усовершенствованного стандарта шифрования (AES).
- TripleDes TripleDes, также известный как 3DES (стандарт тройного шифрования данных), применяет алгоритм DES три раза в каждый блок данных.

Net Security Framework

- Асимметричное шифрование
- Асимметричное шифрование использует пару из двух ключей вместо одного для шифрования. Эти два ключа математически связаны друг с другом. Один из ключей называется открытым ключом, а другой - закрытым.
- ключ. Вы используете один из ключей для шифрования данных и другой для расшифровки данных. Другой ключ должен быть от
- пара ключей, которые вы сгенерировали. Шифрование, которое вы делаете с этими ключами, является взаимозаменяемым. Например, если key1
- зашифровывает данные, тогда key2 может расшифровать их, и если key2 зашифрует данные, то key1 может расшифровать их, потому что один
- из них могут быть переданы каждому, а другой должен храниться в секрете.
- Данные шифруются открытым ключом получателя и могут быть расшифрованы только закрытым ключом.
- от конкретного получателя, потому что только этот пользователь должен иметь доступ к закрытому ключу.
- Открытый ключ передается по данным, в то время как секретный ключ хранится у получателя.
- Асимметричное шифрование позволяет избежать совместного использования ключа шифрования; поэтому он более безопасен, чем симметричный
- ключ. Но, с другой стороны, это медленнее, чем симметричное шифрование.
- .NET Framework предоставляет несколько асимметричных алгоритмов для работы.

Net Security Framework

- RSA - это асимметричный алгоритм, обычно используемый современными компьютерами.
- DSA (алгоритм цифровой подписи), разработанный NIST, является стандартом для создания цифровых
- подписи для целостности данных.
- ECDsa (электронная кривая эллиптической кривой) предлагает вариант DSA.
- ECDiffieHellman Предоставляет базовый набор операций, которые должны поддерживать реализации ECDH

Net Security Framework

- Метод ToXmlString возвращает открытый или закрытый ключ на основе логического значения. Для генерации
- закрытый ключ делает значение истинным, а для открытого ключа значение должно быть ложным.
- Теперь у нас есть два взаимосвязанных ключа асимметричного алгоритма. Если A хочет отправить данные в B, то оба
- стороны должны иметь представление о схеме или ключах, используемых для связи между ними.
- Получатель (B) должен иметь закрытый ключ для расшифровки, а отправитель (A) будет шифровать данные, используя
- открытый ключ. Данные, отправленные в B, будут расшифрованы только с помощью секретного ключа, сгенерированного
- с открытым ключом (используется для шифрования).