

## **ЛЕКЦИЯ №14**

Москва, 2019

## Термины

Гит (Git) — система контроля версий, хранит все изменения в проекте с момента начала, с возможностью вернуться к любому изменению в прошлом;

Звездочки (Stars) — аналог лайка на Фейсбуке (чем больше, тем лучше);

Фолловеры (Followers) — люди, которые подписались на обновления;

Контрибьюторы (Contributors)- люди, которые участвуют в разработке проекта;

Форк (Fork) — копия репозитория на Гитхабе;

Ветка (Branch) — используется для разработки обособленных задач;

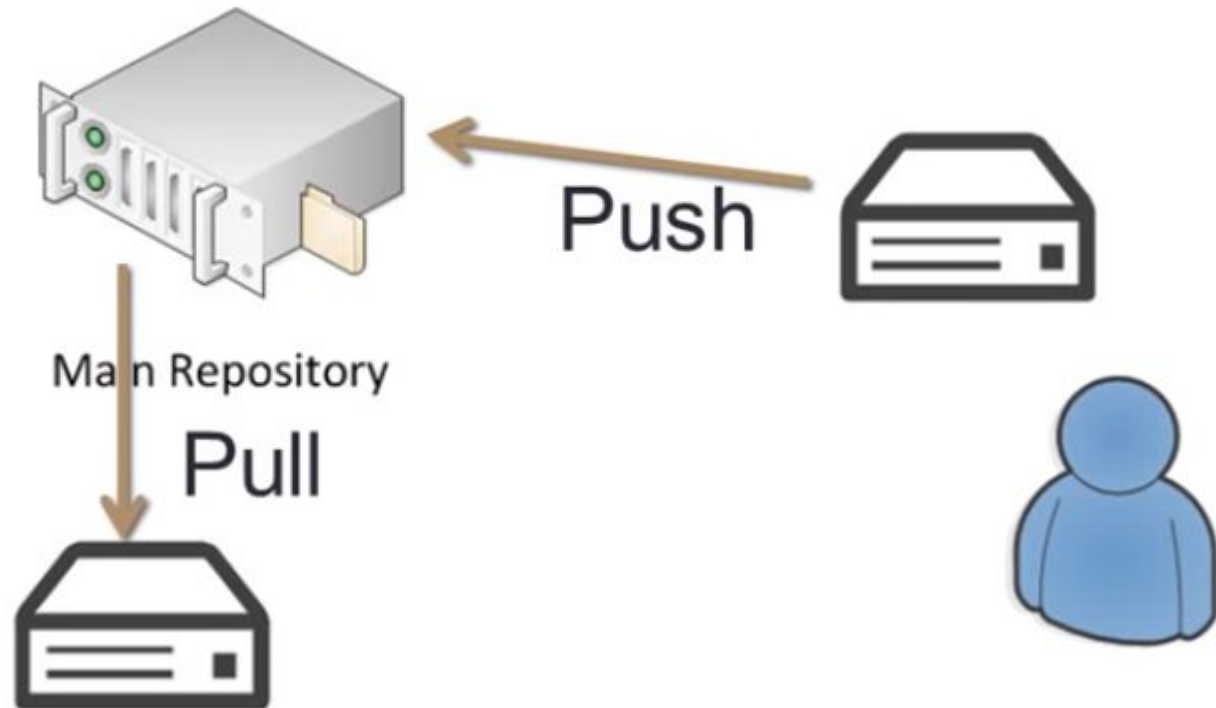
Мердж (Merge) — процесс вливания одной ветки в другую;

Коммит (Commit) — запись изменений в репозиторий;

Код ревью (Code review) — проверка кода на соответствие требованиям, задачам и оформлению;

Пулл реквест (Pull request)— если вы что-то изменили в своем форке и хотите теперь добавить изменения в исходный репозиторий, нужно

# Pushing / Pulling



# SSH

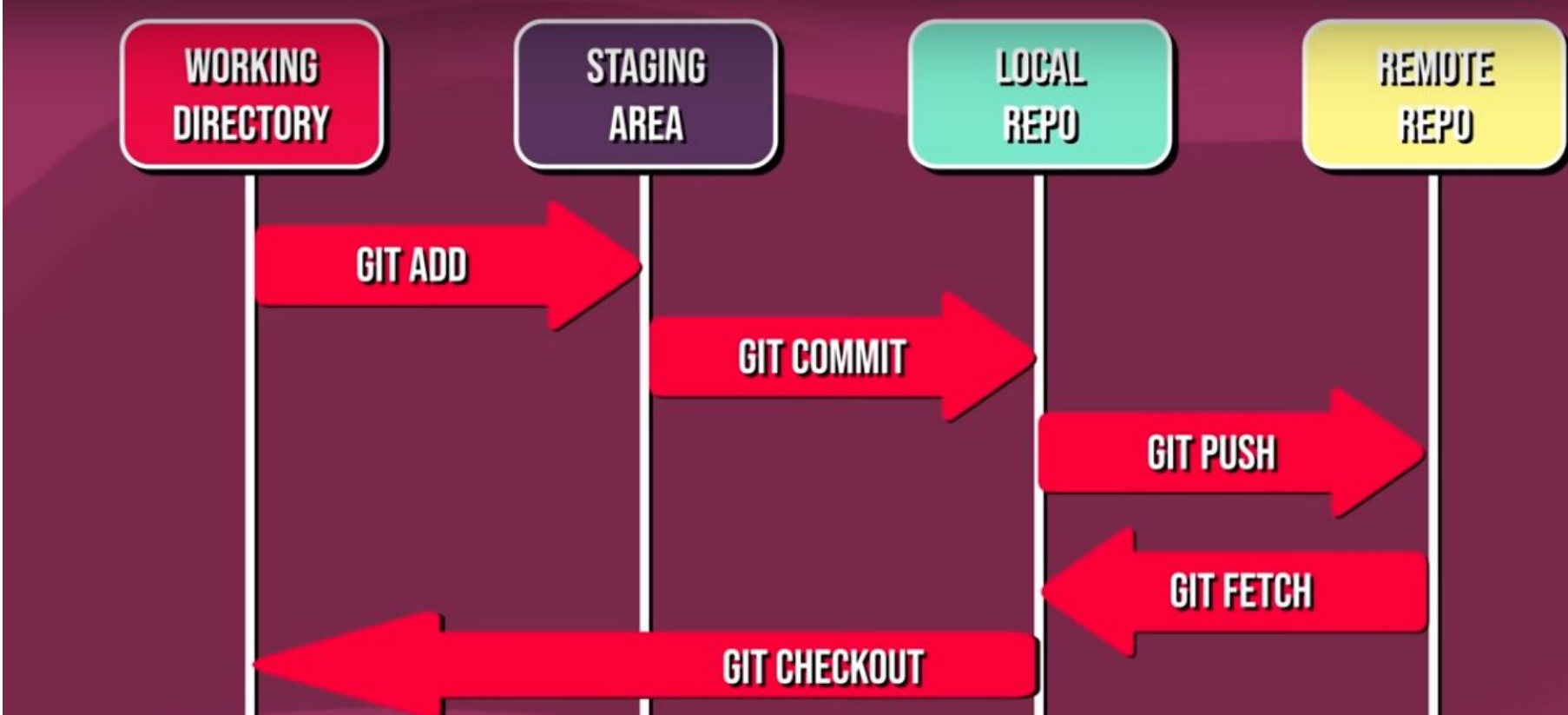
Uses public key cryptography to authenticate who you are.

Two parts:

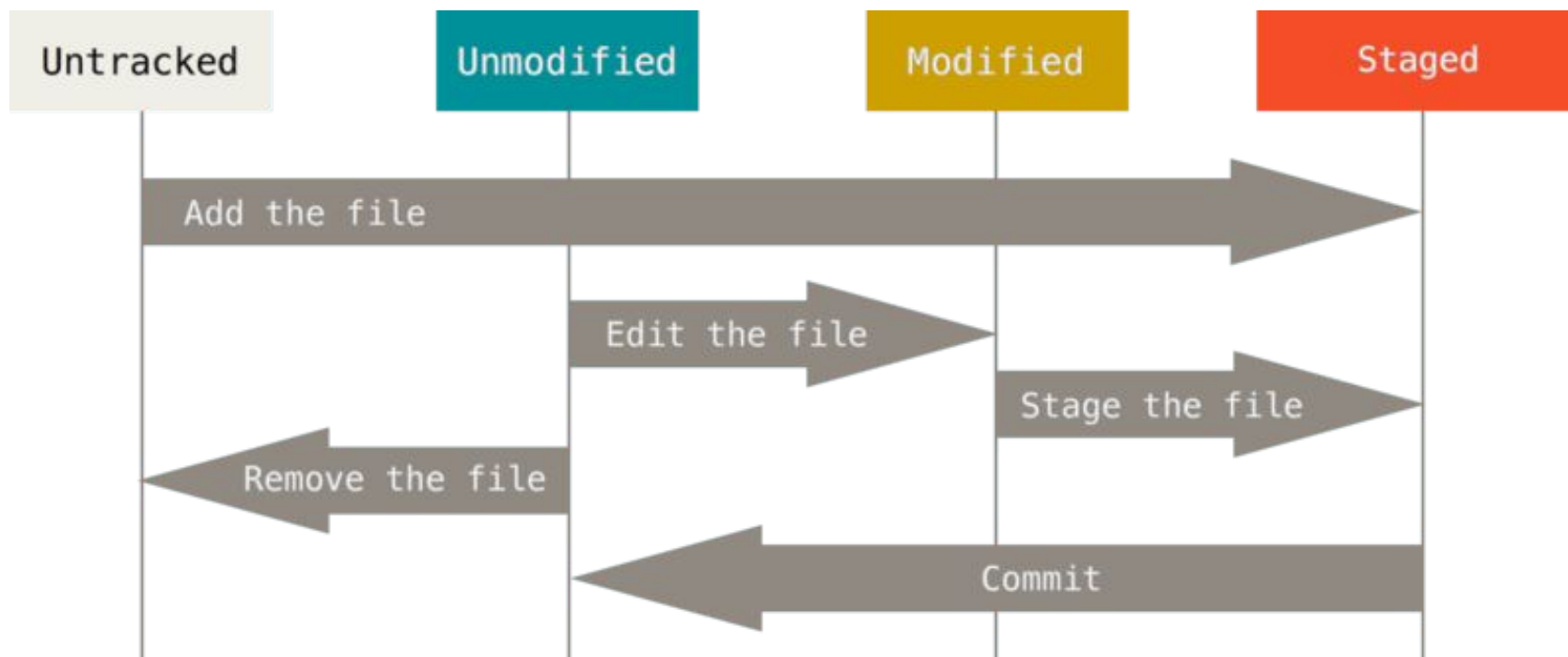


- Public Key – Can share freely
- Private Key – Keep secret!

You can authenticate you are who you claim to be



## Жизненный цикл состояний файлов





### **Live Version**

2017 version that is on market



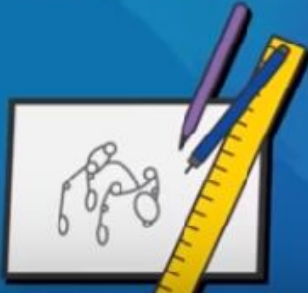
### **Remote Repo**

Current team plans for 2018 version



### **Local Repo**

My latest, improved body design, yet to be okayed by team



### **Staging Area**

A design that I am excited about that still needs testing



### Live Version

2017 version that is on market

Big annual release  
**Deploy**



### Remote Repo

Current team plans for 2018 version

Present to the team  
**Push**



### Local Repo

My latest, improved body design, yet to be okayed by team

Testing process  
**Commit**



### Staging Area

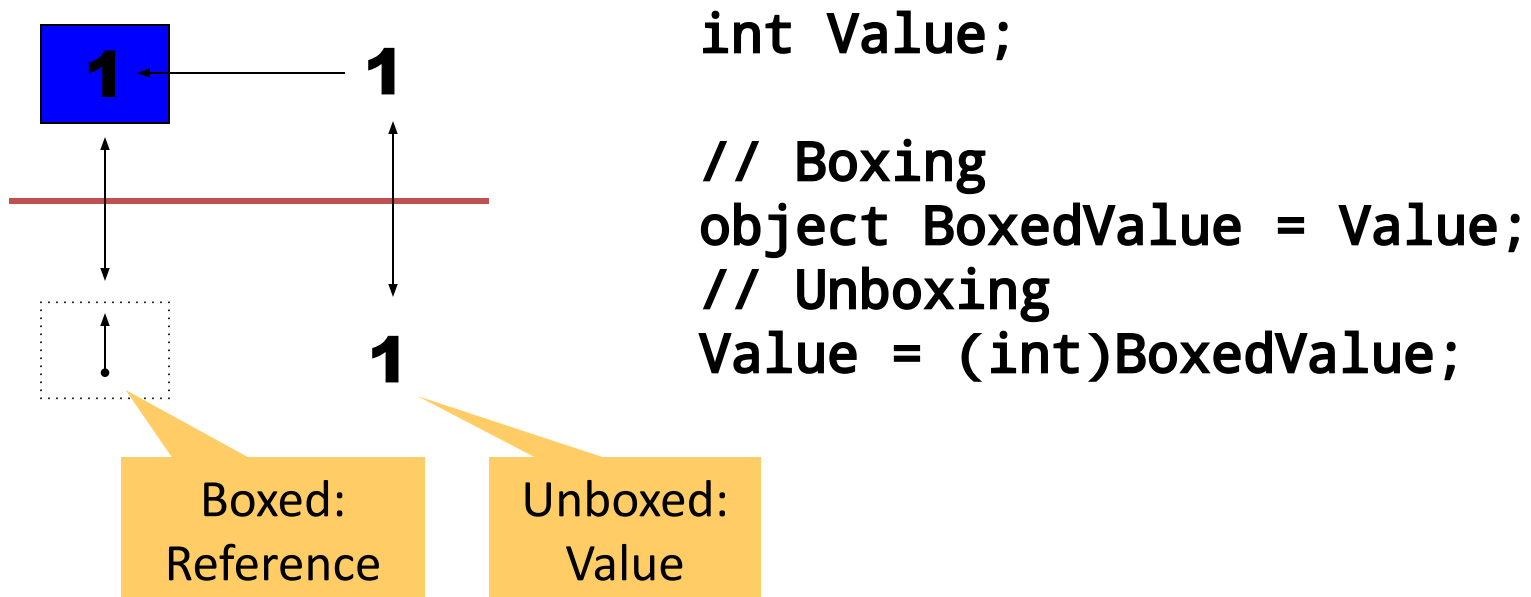
A design that I am excited about that still needs testing

Initial Design Process



# 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-оберткок”)
- Boxing / unboxing *не является CLS-совместимой операцией*
- Java 1.5: Sun решил ввести boxing и unboxing в Java (наряду с классами-обертками)



# 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