**План**

1. Кратко об HTTP
2. Проблемы безопасности HTTP
3. HTTPS
4. TLS
5. Cнифферские атаки
6. Man-in-the-middle атаки
7. Принцип работы HTTPS
8. Симметричные криптосистемы
9. Асимметричная схема шифрования (криптосистема с открытым ключом)

* Проблемы безопасности

1. Симметричные криптосистемы

Конспект

4. TLS

1. На данный момент актуальные версии протокола TLS это версии не ниже 1.2 (1.2 и 1.3).

Версия 1.2 использует криптографический алгоритм RSA, на замены которого в версии 1.3 пришёл более продвинутый алгоритм DH (алгоритм обмена ключами Ди́ффи — Хе́ллмана).

* Недостатки алгоритм RSA: Доступ к секретному ключу позволит расшифровать все передаваемые (переданные) данные.
* Уязвим для атак Million message attack (атаки миллиона сообщений) и ROBOT (Return Of Bleichenbacher's Oracle Threat)