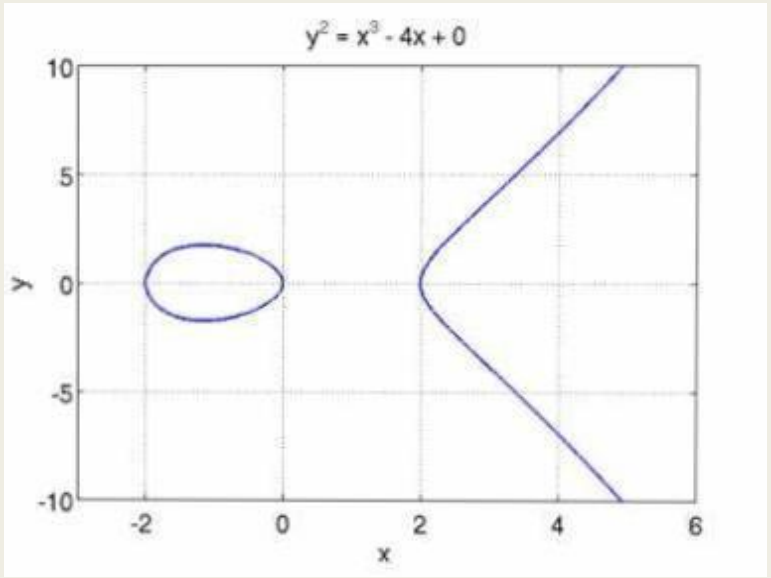
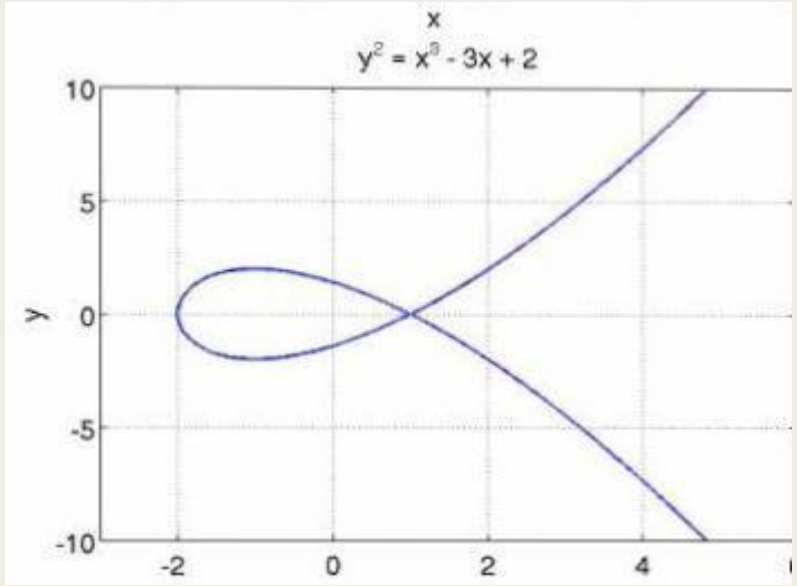
ЭЛЛИПТИЧЕСКАЯ КРИПТОГРАФИЯ

Уфимский колледж статистики, информатики и вычислительной техники
Головина Анна Владимировна
17И-2, 2019 г.

Понятие эллиптических кривых

- Эллиптические кривые- это множество точек, удовлетворяющих уравнению: y^3=x^2+ax+b
- В криптографии используют исключительно гладкие кривые, для которых выполняется неравенство: 4a^3+ 27b^2=/=0





Области применения эллиптической криптографии

- Протоколы TLS и SSH
- Цифровая подпись и шифрование- PGP
- Правительственные службы для внутренней коммуникации
- Обеспечение совершенной прямой секретности (PFS)
- Т.д.

Основные плюсы эллиптической криптографии

- Меньшая длина ключа
- Высокая скорость работы алгоритмовв шифрования
- Возможность использования на устройствах с ограниченными вычислительными ресурсами

	RSA-1024	ECC-168
Длина открытого **ключа**, битов	1024	169
Скорость генерации **ключа**, мс	1432	65
Скорость шифрования, мс	4,28	140
Скорость расшифрования, мс	48,5	67

Основные минусы эллиптической криптографии

- Сложность понимая шифрования
- Отсутвиие алгоритма решения задачи дискретного логарифмирования на эллиптических кривых

Итоги

- Эллиптическая криптография — раздел криптографии, который изучает асимметричные криптосистемы, основанные на эллиптических кривых над конечными полями.
- Шифрование на основе эллиптических кривых обеспечивает абсолютную безопасность
- В случае нахождения алгоритма дешифровки- обвалятся все криптосистемы