

The background is a dark blue gradient with a starry texture. On the left side, there are several overlapping circular elements. A prominent one is a large circle with a scale from 140 to 260 in increments of 10. Other circles are smaller and some have dashed outlines. There are also curved arrows and partial circles scattered throughout the left half of the image.

# СОВРЕМЕННЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ

# ГОСУДАРСТВЕННЫЙ СТАНДАРТ ШИФРОВАНИЯ В РОССИИ

- Государственным стандартом шифрования в России является ГОСТ 28147-89
- Он является блочным шифром

# СТАНДАРТ ШИФРОВАНИЯ В США

- В США в качестве стандарта используется блочный шифр AES(Advanced Encryption Standard , передовой стандарт шифрования) принятый в 2001г. Так же он используется в сетях Wi-Fi

# АЛГОРИТМ RSA

- Алгоритм RSA назван первыми буквами фамилий его создателей (R. Rivest, A. Shamir, L. Adleman).
- Это алгоритм с открытым ключом.
- Его стойкость основана на том, что перемножить два очень больших простых числа просто, а разложить такое произведение на простые сомножители – очень трудно и решить такую задачу возможно только путем длительного перебора.

# ПРЕИМУЩЕСТВА RSA

- Стойкость
- Его можно использовать для создания цифровой подписи

# ЦИФРОВАЯ ПОДПИСЬ

- Цифровая подпись – это набор символов, который получен в результате шифрования сообщения с помощью секретного личного кода отправителя

