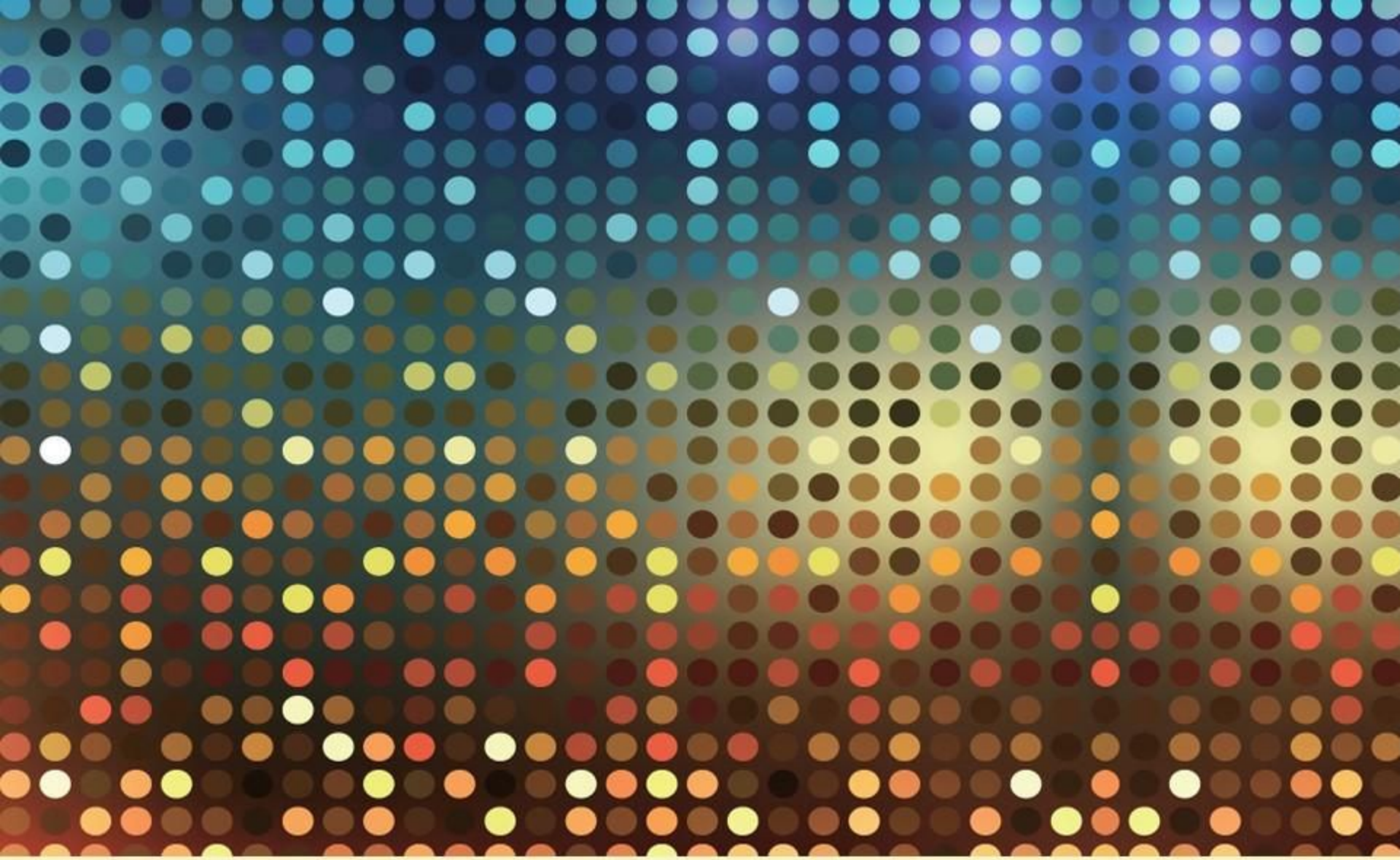


ИСТОРИЯ КРИПТОГРАФИИ

- История криптографии насчитывает около 4 тысяч лет.

- В качестве основного критерия периодизации криптографии возможно использовать технологические характеристики используемых методов шифрования.

Первый период

- Приблизительно с 3-го тысячелетия до н. э.

Характеризуется господством моноалфавитных шифров

Основной принцип — замена алфавита исходного текста другим алфавитом через замену букв другими буквами или символами.

Примеры: Атбаш, шифр Цезаря, Литорея.

Второй период

- С IX века на Ближнем Востоке и с XV века в Европе — до начала XX века

Ознаменовался введением в обиход полиалфавитных шифров.

Суть заключается в циклическом применении нескольких моноалфавитных шифров к определённому числу букв шифруемого текста.

Примеры: шифр Вижинера, шифр Гронсфельда.

Третий период

- С начала и до середины XX века

Характеризуется внедрением электромеханических устройств в работу шифровальщиков.

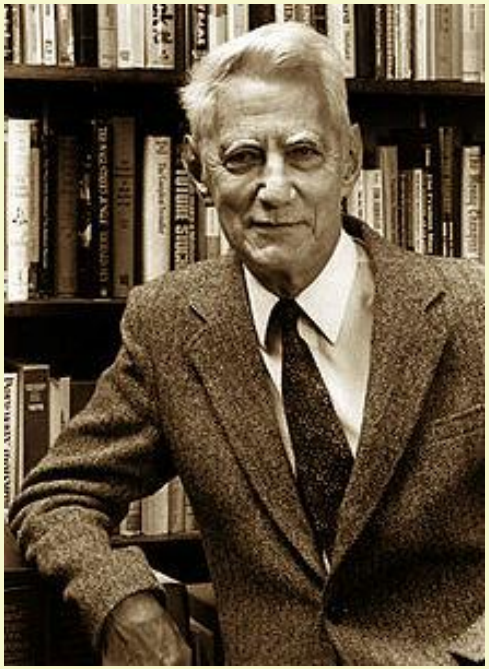
Эти устройства делились на два типа — роторные машины и машины на цевочных дисках.

Примеры: «Энигма», Машина Лоренца, М-209.

Четвёртый период

- С середины до 70-х годов XX века

- период перехода к математической криптографии.



Фундаментальный труд Клода Шенона «*Теория связи в секретных системах*». В этой работе, был впервые показан подход к криптографии в целом как к математической науке.

Интересные факты:

- Слово криптография произошло от названия подземных помещений, которые использовались для секретных встреч, собраний заговорщиков, работы над шифрами и т.п.
  Греки называли их "спрятанные".

Интересные факты:

- Первый шифровальный прибор был изобретенный в Древней Спарте. Для шифрования текста использовался цилиндр, на который наматывалась пергаментная лента и писался текст.

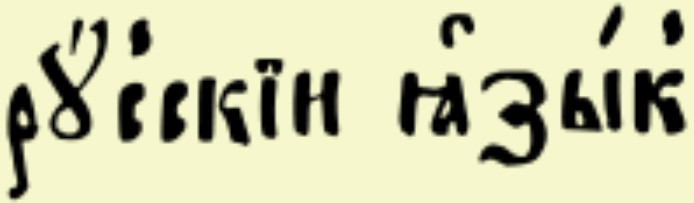
«Скитала»

Интересные факты:

- Георг Фридрих Гротефенд прославился, расшифровав знаменитую Персепольскую надпись, содержащую родословные и списки подвигов персидских владык. С помощью гениальной догадки, он расшифровал всего одно слово - *царь*, а дальнейшее уже было делом техники.

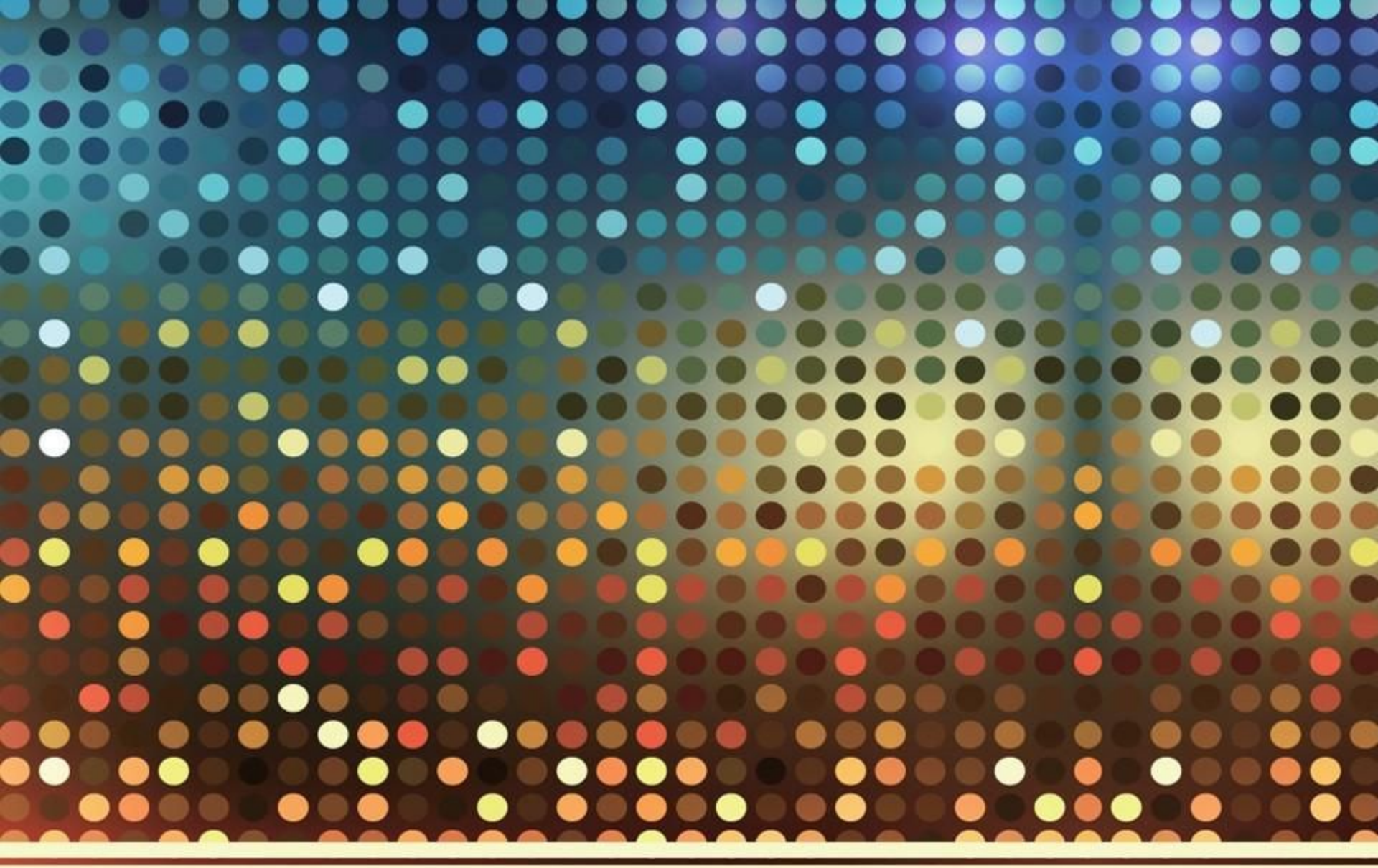
Интересные факты:

- Немцы перехватывали немало важных сообщений. Сделать коды партизан неуязвимыми для педантичных немцев помогали орфографические ошибки. Оказывается, сообщения с орфографическими ошибками ставили в тупик вражеских дешифровальщиков, которые педантично руководствовались правилами русского языка.



Интересные факты:

- В обеих мировых войнах американцам удавалось обеспечить секретность связи, хотя у немцев были радиоперехваты, но ни им, ни японцам не удалось расшифровать тексты. Радистами на флоте США служили индейцы, которые общались без шифра на своем родном языке.



Выполнил ученик 10 «А» класса :

Иванов И.