

Старт в DevOps: системное администрирование для начинающих

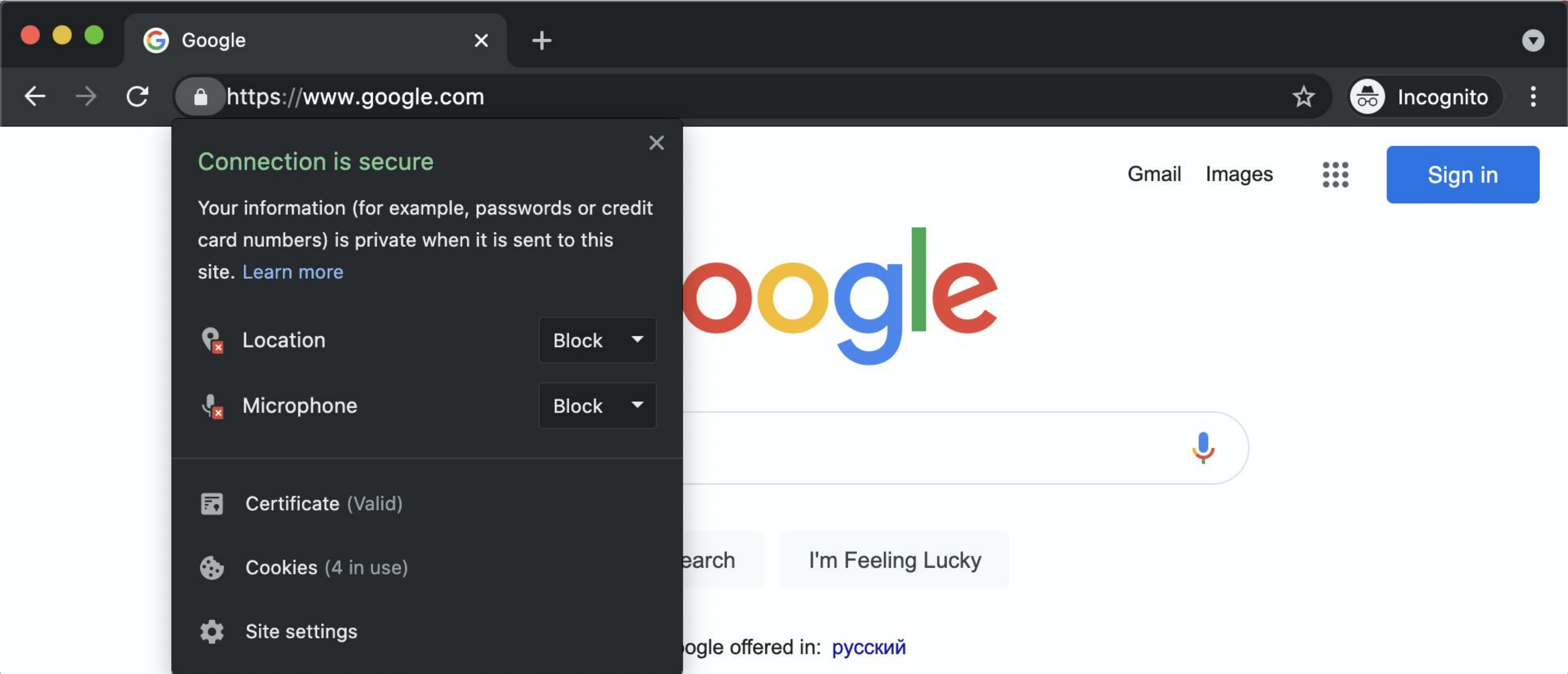
Виктория Маркова

Lead DevOps
«Валарм»

Криптография. HTTPS

Разбор домашнего задания

Основные понятия криптографии



Плюсы https

- Защита взаимодействия пользователя с веб-ресурсом от перехвата
- Защита взаимодействия пользователя с веб-ресурсом от изменения
- Подтверждение аутентичности сайта

”

Криптография — это наука о методах обеспечения конфиденциальности, целостности данных, аутентификации и шифрования.

Хэш-функция



Исходный текст

Хэш-функция



5165bfe658c15afd5a6d8d6db6146486

Строка фиксированной длины

Определения

- **Открытый (исходный) текст** — обычные, незашифрованные данные
- **Шифр, криптосистема** — семейство обратимых преобразований открытого текста в зашифрованный
- **Шифротекст, зашифрованный (закрытый) текст, криптограмма** — данные, полученные после применения криптосистемы (шифра)
- **Ключ** — параметр шифра, определяющий выбор конкретного преобразования данного текста
- **Шифрование** — процесс применения криптографического преобразования открытого текста на основе алгоритма и ключа, в результате которого возникает зашифрованный текст
- **Расшифровывание** — процесс нормального применения криптографического преобразования зашифрованного текста в открытый

Шифры перестановки

Скитала



Шифр маршрутной перестановки

Открытый текст: ПРИМЕРМАРШРУТНОЙПЕРЕСТАНОВКИ

П	Р	И	М	Е	Р	М
Н	Т	У	Р	Ш	Р	А
О	Й	П	Е	Р	Е	С
И	К	В	О	Н	А	Т

Зашифрованный текст: МАСТАЕРРЕШРНОЕРМИУПВКЙТРПНОИ

Шифры подстановки

Шифр Цезаря

Исходный алфавит:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Алфавит замены:

E F G H I J K L M N O P Q R S T U V W X Y Z A B C D



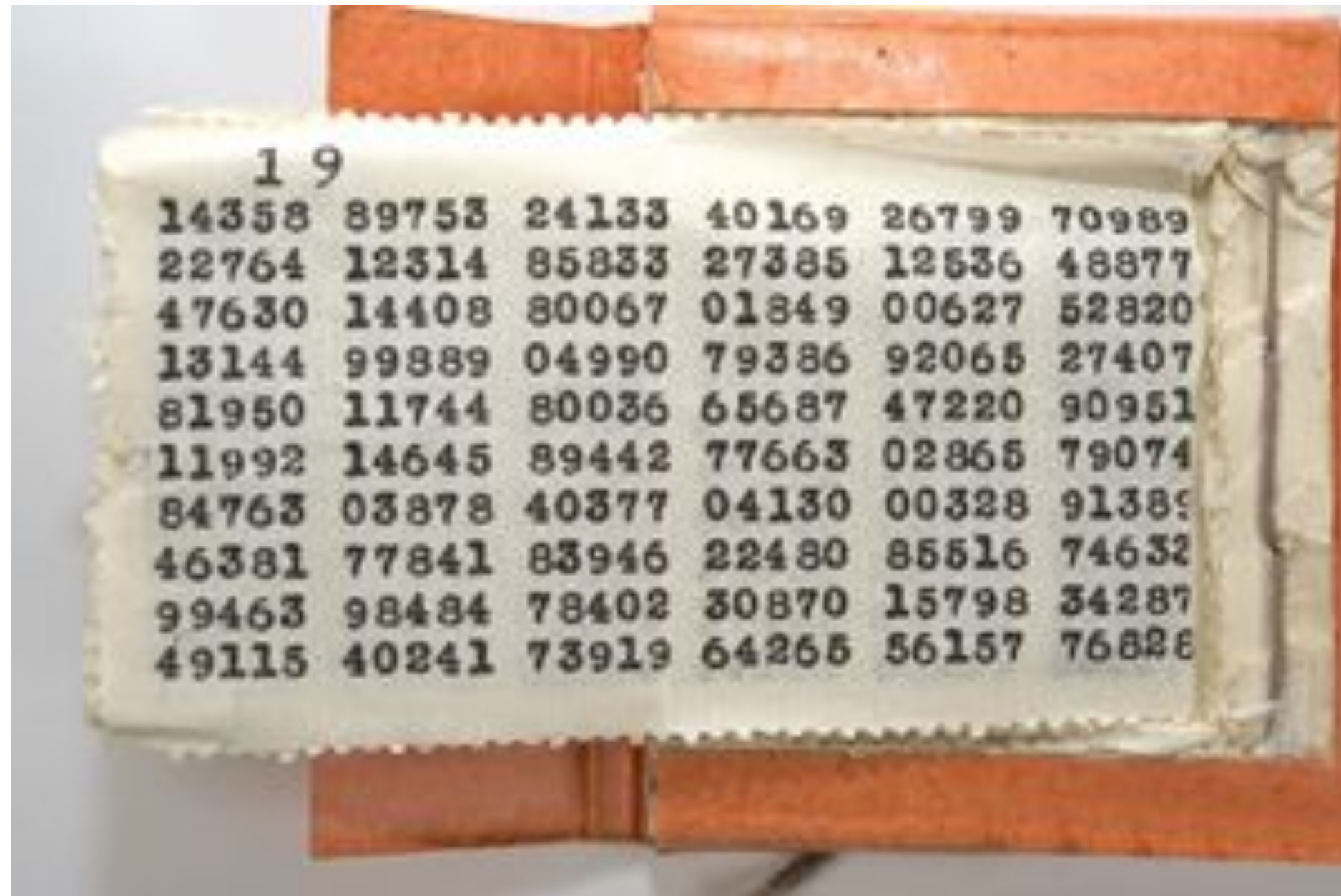
Шифр Виженера

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Исходный текст: ATTACKATDAWN

Ключ: LEMONLEMONLE

Зашифрованный текст: LXFOPVEFRNHR



1	9				
14358	89753	24133	40169	26799	70989
22764	12314	85833	27385	12536	48877
47630	14408	80067	01849	00627	52820
13144	99889	04990	79386	92065	27407
81950	11744	80036	65687	47220	90951
11992	14645	89442	77663	02865	79074
84763	03878	40377	04130	00328	91389
46381	77841	83946	22480	85516	74632
99463	98484	78402	30870	15798	34287
49115	40241	73919	64265	56157	76828

Спасибо за внимание!