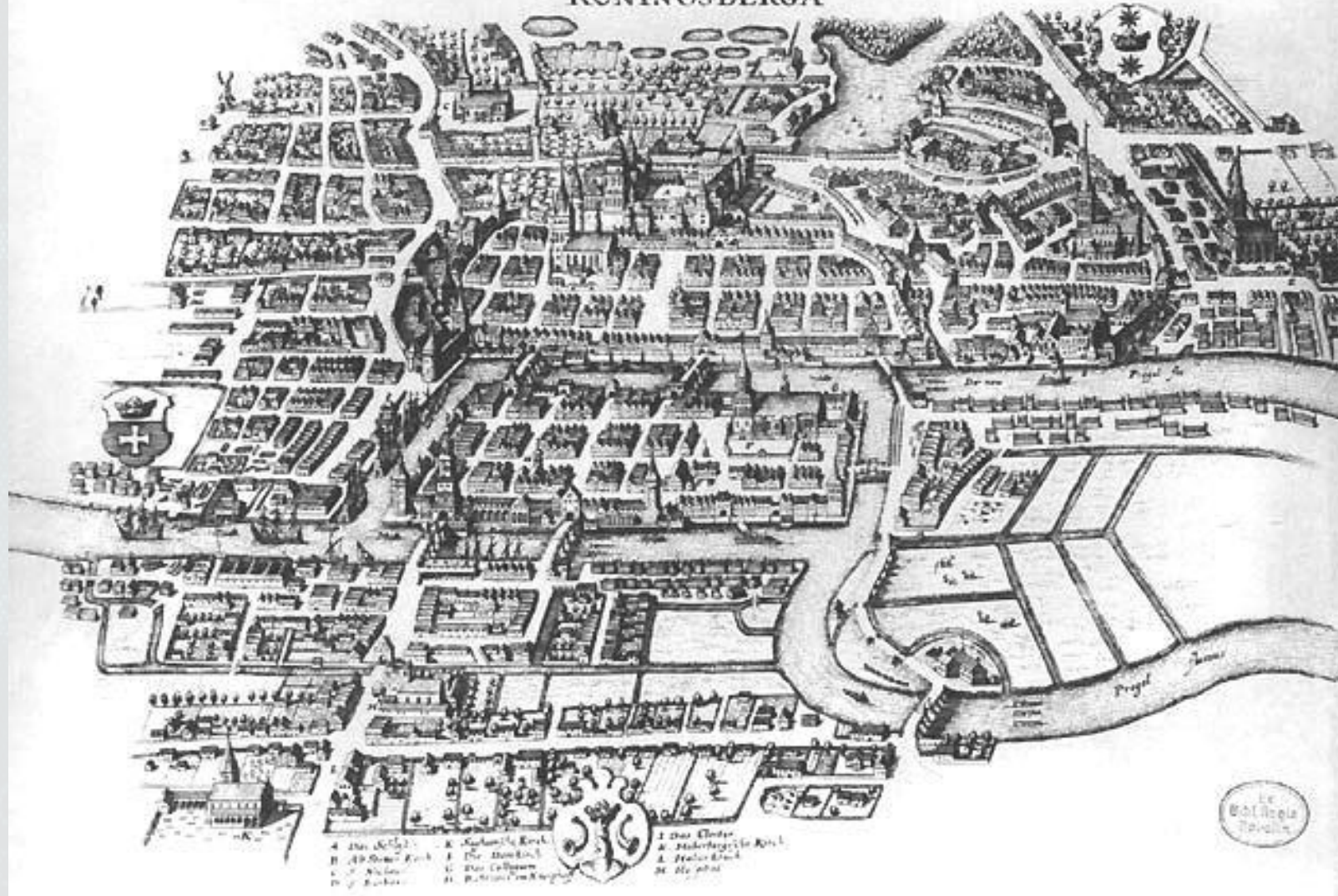
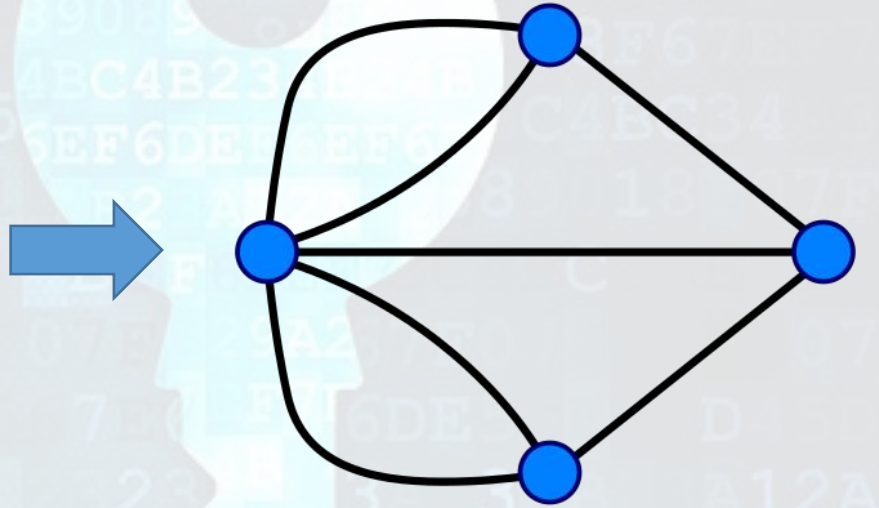
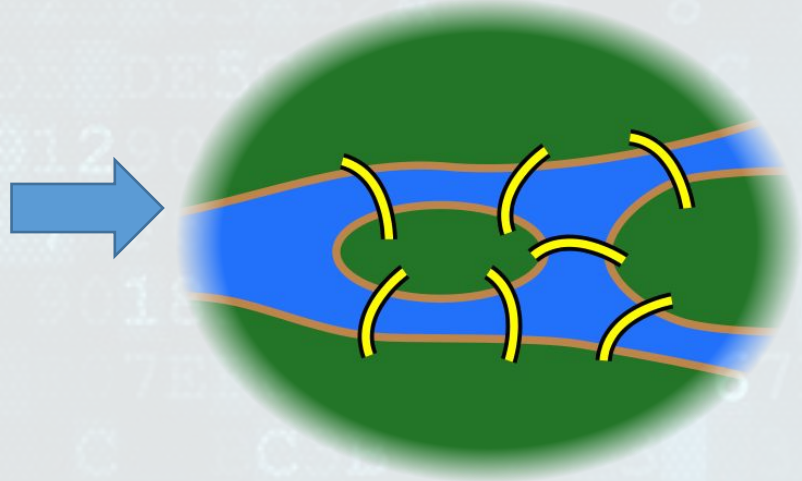
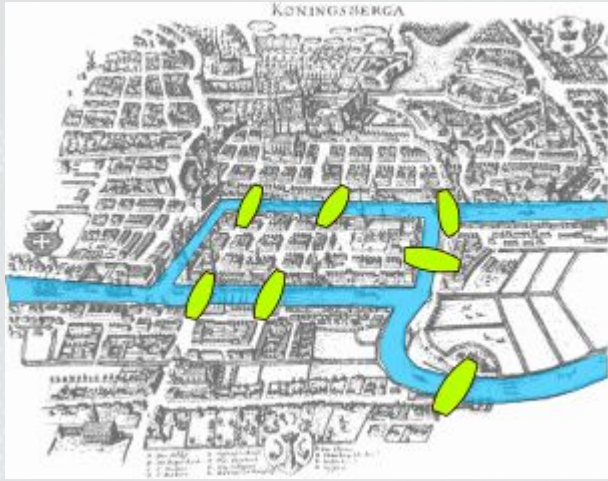


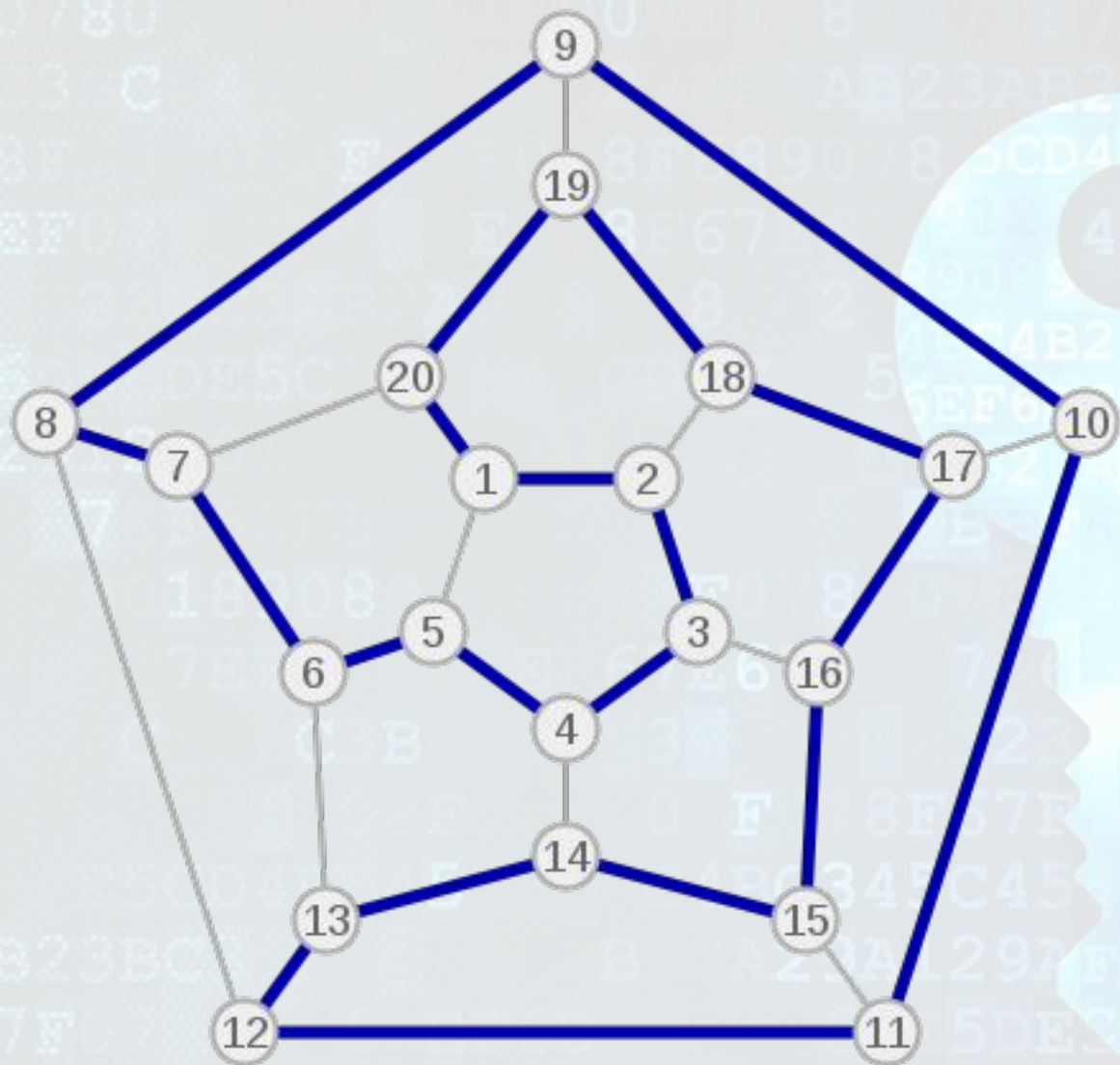
Игра в имитацию



KONINGSBERGA









Шифр Цезаря



а	б	в	г	...	ь	э	ю	я
↓	↓	↓	↓	...	↓	↓	↓	↓
г	д	е	ё	...	я	а	б	в



Частотность букв

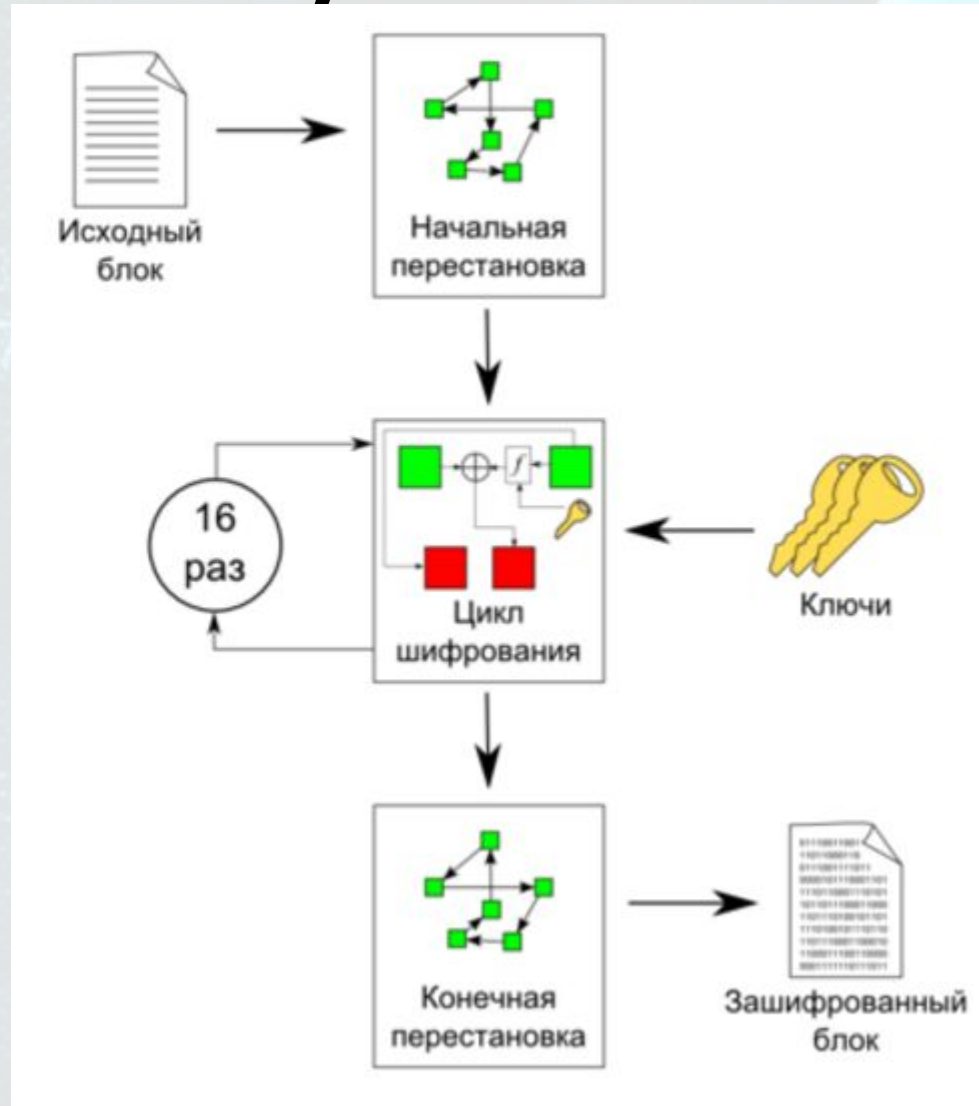
а	б	в	г	д	е,ё	ж	з	и	й	к	л	м	н	о	п	р	с	т
0.075	0.017	0.046	0.016	0.03	0.087	0.009	0.018	0.075	0.012	0.034	0.042	0.031	0.065	0.110	0.028	0.048	0.055	0.065
у	ф	х	ц	ч	ш	щ	ъ,ь	ы	э	ю	я							
0.025	0.002	0.011	0.005	0.015	0.007	0.004	0.017	0.019	0.003	0.007	0.022							

Ход конец

12	9	20	20	22	5	4	16	3	17	1	5	8						
9	12	9	11	6	13	11	13	9	23	11	5	8	16	5	;			
9	11	12	8	2	4	17	8	19	13	10	14	22	7	17	21	14	16	.
12	18	20	17	7	5	11	14	2	22	5	9	12	8	8	16	13	6	12
16	9	12	5	19	14	4	9	12	10	9	12	12	11	4	.			

1	А	2	Б	3	В
Г	4	Д	5	Е	6
7	И	8	Й	9	К
Л	10	Н	11	О	12
13	П	14	Р	15	С
Т	16	У	17	Х	18
19	Ч	20	Щ	21	Ы
Ь	22	Я	23		24

Симметричное шифрование (закрытый ключ)



Асимметричное шифрование (открытый ключ)

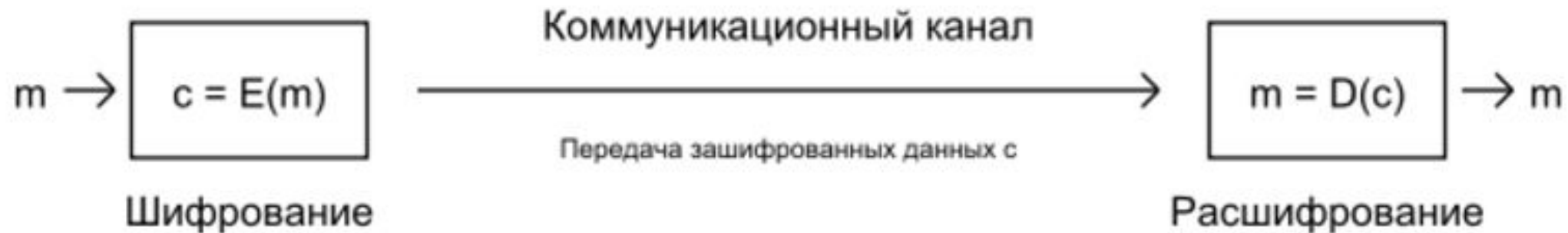


Боб

есть открытый ключ Алисы

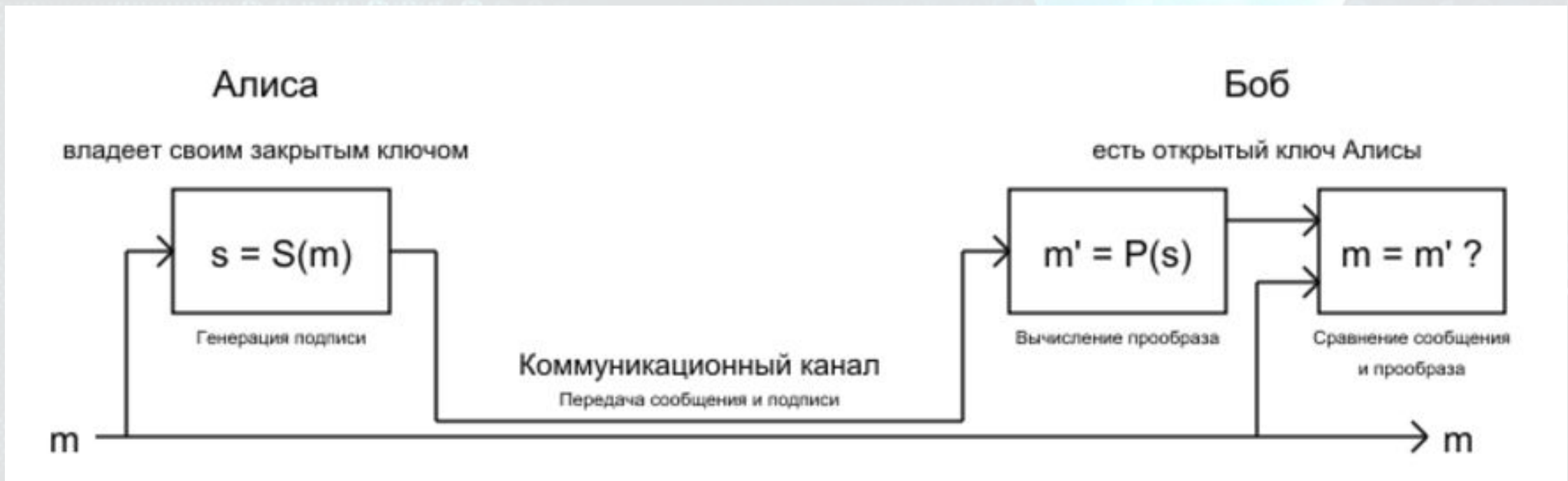
Алиса

владеет своим закрытым ключом



Этап	Описание операции	Результат операции
Генерация ключей	Выбрать два простых различных числа	$p = 3557,$ $q = 2579$
	Вычислить произведение	$n = p \cdot q = 3557 \cdot 2579 = 9173503$
	Вычислить функцию Эйлера	$\varphi(n) = (p - 1)(q - 1) = 9167368$
	Выбрать открытую экспоненту	$e = 3$
	Вычислить секретную экспоненту	$d = e^{-1} \pmod{\varphi(n)}$ $d = 6111579$
	Опубликовать <i>открытый</i> ключ	$\{e, n\} = \{3, 9173503\}$
	Сохранить <i>закрытый</i> ключ	$\{d, n\} = \{6111579, 9173503\}$
Шифрование	Выбрать текст для зашифрования	$m = 111111$
	Вычислить шифртекст	$c = E(m)$ $= m^e \pmod{n}$ $= 111111^3 \pmod{9173503}$ $= 4051753$
Расшифрование	Вычислить исходное сообщение	$m = D(c) =$ $= c^d \pmod{n}$ $= 4051753^{6111579} \pmod{9173503}$ $= 111111$

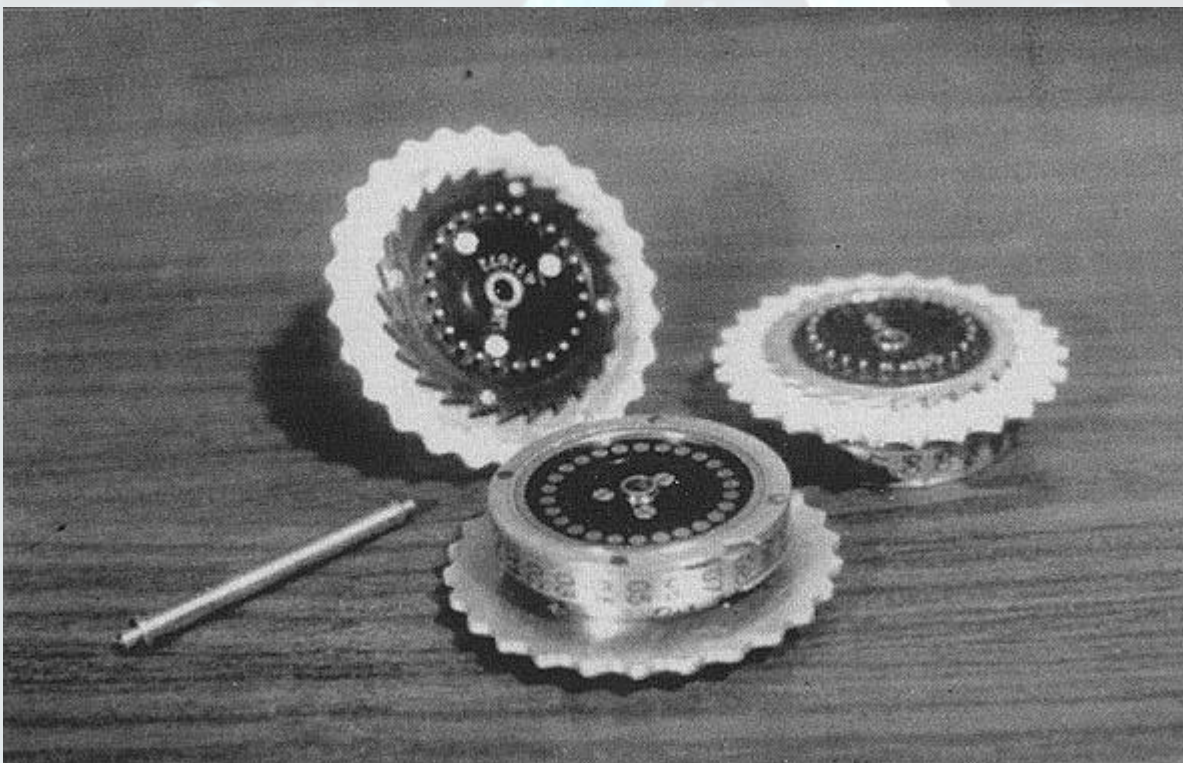
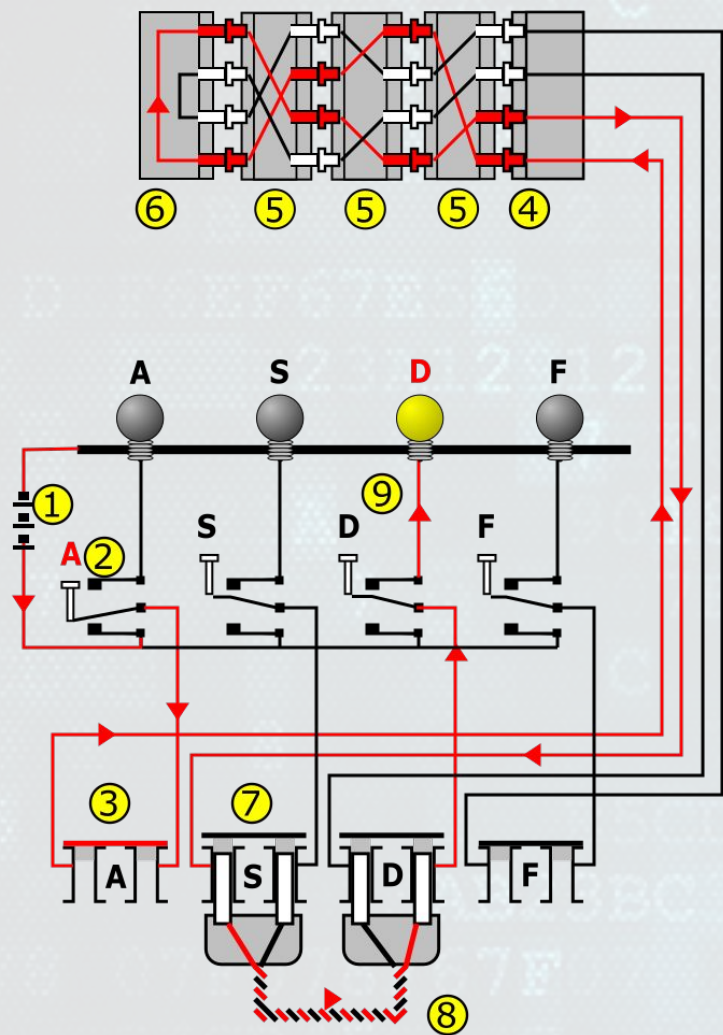
Цифровая ПОДПИСЬ



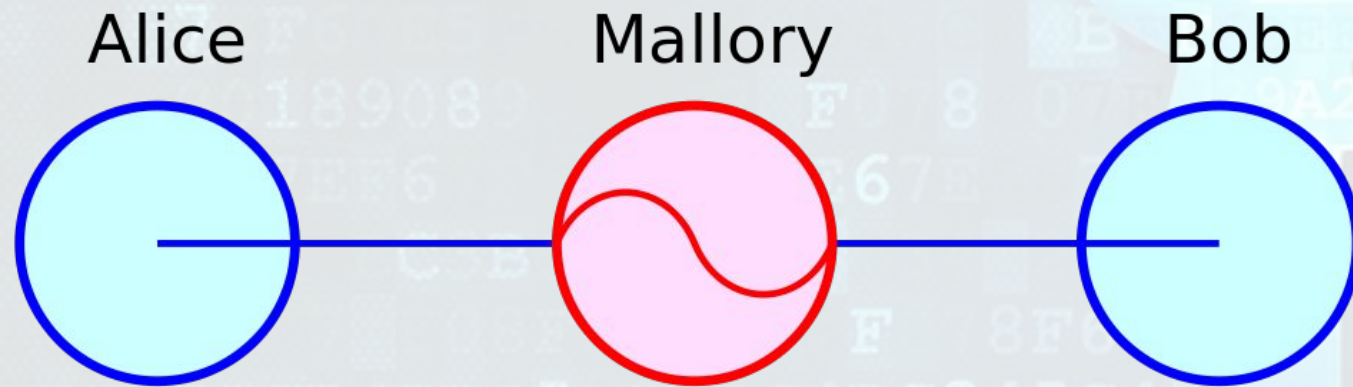
ЭНИГМ

а





Атака «человек посередине»



Криптограмма Бэйла

THE
BEALE PAPERS,
CONTAINING
AUTHENTIC STATEMENTS
REGARDING THE
TREASURE BURIED
IN
1819 AND 1821,
NEAR
BUFORDS, IN BEDFORD COUNTY, VIRGINIA,
AND
WHICH HAS NEVER BEEN RECOVERED.

PRICE FIFTY CENTS.

LYNCHBURG:
VIRGINIAN BOOK AND JOB PRINT,
1881.

71, 194, 38, 1701, 89, 76, 11, 83, 1629, 48, 94, 63, 132, 16, 111, 95, 84, 341, 975,
14, 40, 64, 27, 81, 139, 213, 63, 90, 1120, 8, 15, 3, 126, 2018, 40, 74, 758, 485,
604, 230, 436, 664, 582, 150, 251, 284, 308, 231, 124, 211, 486, 225, 401, 370,
11, 101, 305, 139, 189, 17, 33, 88, 208, 193, 145, 1, 94, 73, 416, 918, 263, 28, 500,
538, 356, 117, 136, 219, 27, 176, 130, 10, 460, 25, 485, 18, 436, 65, 84, 200, 283,
118, 320, 138, 36, 416, 280, 15, 71, 224, 961, 44, 16, 401, 39, 88, 61, 304, 12, 21,
24, 283, 134, 92, 63, 246, 486, 682, 7, 219, 184, 360, 780, 18, 64, 463, 474, 131,
160, 79, 73, 440, 95, 18, 64, 581, 34, 69, 128, 367, 460, 17, 81, 12, 103, 820, 62,
116, 97, 103, 862, 70, 60, 1317, 471, 540, 208, 121, 890, 346, 36, 150, 59, 568,
614, 13, 120, 63, 219, 812, 2160, 1780, 99, 35, 18, 21, 136, 872, 15, 28, 170, 88, 4,
30, 44, 112, 18, 147, 436, 195, 320, 37, 122, 113, 6, 140, 8, 120, 305, 42, 58, 461,
44, 106, 301, 13, 408, 680, 93, 86, 116, 530, 82, 568, 9, 102, 38, 416, 89, 71, 216,
728, 965, 818, 2, 38, 121, 195, 14, 326, 148, 234, 18, 55, 131, 234, 361, 824, 5,
81, 623, 48, 961, 19, 26, 33, 10, 1101, 365, 92, 88, 181, 275, 346, 201, 206, 86,
36, 219, 324, 829, 840, 64, 326, 19, 48, 122, 85, 216, 284, 919, 861, 326, 985,
233, 64, 68, 232, 431, 960, 50, 29, 81, 216, 321, 603, 14, 612, 81, 360, 36, 51, 62,
194, 78, 60, 200, 314, 676, 112, 4, 28, 18, 61, 136, 247, 819, 921, 1060, 464, 895,
10, 6, 66, 119, 38, 41, 49, 602, 423, 962, 302, 294, 875, 78, 14, 23, 111, 109, 62,
31, 501, 823, 216, 280, 34, 24, 150, 1000, 162, 286, 19, 21, 17, 340, 19, 242, 31,
86, 234, 140, 607, 115, 33, 191, 67, 104, 86, 52, 88, 16, 80, 121, 67, 95, 122, 216,
548, 96, 11, 201, 77, 364, 218, 65, 667, 890, 236, 154, 211, 10, 98, 34, 119, 56,
216, 119, 71, 218, 1164, 1496, 1817, 51, 39, 210, 36, 3, 19, 540, 232, 22, 141, 617,
84, 290, 80, 46, 207, 411, 150, 29, 38, 46, 172, 85, 194, 39, 261, 543, 897, 624, 18,
212, 416, 127, 931, 19, 4, 63, 96, 12, 101, 418, 16, 140, 230, 460, 538, 19, 27, 88,
612, 1431, 90, 716, 275, 74, 83, 11, 426, 89, 72, 84, 1300, 1706, 814, 221, 132,
40, 102, 34, 868, 975, 1101, 84, 16, 79, 23, 16, 81, 122, 324, 403, 912, 227, 936,
447, 55, 86, 34, 43, 212, 107, 96, 314, 264, 1065, 323, 428, 601, 203, 124, 95, 216,
814, 2906, 654, 820, 2, 301, 112, 176, 213, 71, 87, 96, 202, 35, 10, 2, 41, 17, 84,
221, 736, 820, 214, 11, 60, 760.

Внимание: конкурс!

- Вступить в группу
<https://vk.com/crocode>
- Расшифровать криптограмму
- Первым оставить правильный ответ в комментариях под постом
- Получить приз!

Спасибо за внимание!

