1.6.12

Шифртекст:

TNOSSKAIMAGAEITMHETHTSRHXXIHEUXDX

NUEIDSATDTDDSARAHHENTTTDSOUIOEART

FHDAOMWYWFERTNEONFDYAHSEIMEDGRWTA

TISURUARTHJ

|  | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **0** | T | N | O | S | S | K | A | I | M | A | G |
| **1** | A | E | I | T | M | H | E | T | H | T | S |
| **2** | R | H | X | X | I | H | E | U | X | D | X |
| **3** | N | U | E | I | D | S | A | T | D | T | D |
| **4** | D | S | A | R | A | H | H | E | N | T | T |
| **5** | T | D | S | O | U | I | O | E | A | R | T |
| **6** | F | H | D | A | O | M | W | Y | W | F | E |
| **7** | R | T | N | E | O | N | F | D | Y | A | H |
| **8** | S | E | I | M | E | D | G | R | W | T | A |
| **9** | T | I | S | U | R | U | A | R | T | H | J |

Найдём методом Hill Climbing перестановку столбцов. В качестве функции оценки возьмём разницу частот квадграмм. Найдём имя ARTHUR, поймём, что X – это паддинг для сообщения. Повторим до тех пор, пока не получится правильная перестановка столбцов (все X должны быть в конце в строке 2). Найдём перебором или методом Hill Climbing перестановку строк (строка 2 должна быть в конце).

Столбцы=[6, 4, 0, 9, 5, 7, 1, 10, 3, 2, 8]

Строки=(9, 4, 8, 0, 1, 3, 7, 5, 6, 2)

Открытый текст:

ARTHURIJUSTHADTHESTRANGESTDREAMIWASTAKINGSOMEMATHTESTIHADNTSTUDIEDFORANDTHENYOUTRIEDTOSAWOFFMYHEADWEIRDHUHXXXX

ARTHUR, I JUST HAD THE STRANGEST DREAM. I WAS TAKING SOME MATH TEST I HADN’T STUDIED FOR AND THEN YOU TRIED TO SAW OFF MY HEAD! WEIRD, HUH…

(The Tick, Season 1: The Tick vs. the Uncommon Cold)

2.6.5 How many pairs of cycles are required in order to uniquely determine

the Enigma rotor settings?

NumPairs >= log(K)/log(26), K – Enigma Key space ~ 2^30 (26^2\*26^3\*5!/2!) >= 7