

## Breaking a Transposition Cipher

The ciphertext (1066 characters), encrypted using a transposition cipher, with key a permutation of degree 26.<sup>1</sup> For convenience, the ciphertext is written 26 characters per line.

```
FATENCNNHYNONINCODTOEOTIIL
IAETCMETRAOYIAHNCEUSUTDNAN
TRQADHCFUINXTRNEETTHOESENE
ABRAUOASYTIOOWOYMRBFAONRTP
YHOTYFDEFNOTEAONNDOIMHACLW
DHATWETTNMEEIOAMHNHONYASTA
OINLEDRIGSCBSCSTHIOLAHNAWRR
FLAIFNWHMEOOYFDOHOERTUMAHT
ANDAILTAWGDLTIWHEALNMDNEDN
OOMOIDDATDOSEGNFNGNELOAHHL
MNI AHFAEMHEIDODHY PDRPNRORA
TOOFGAWTDOSWRITHAHHEMANTDH
LYALEENTLOAPCMEOENHTEWEPRE
CDYALMTOMENAFRAOAIYNJURERQ
DGSUEKTNHSEEGDCEHHDOAASICE
YRNCARHVDOLDIDOEKEAEOBYRT
RNAADNDHYOOWDIHHPAANGCLDII
DSFARDNNECAETDDEGSDAANNAOA
DVGTDLEEOATNEYERP YLKMHWONT
IPIUHSOASDENFRTOGSYTDHNATG
SYEBHDTORWOADYIATGNHLSNOTA
WTEIENFBWROSHAIGRNAGYVENS A
OYVREYPOEDNHBLEAATNOC SNAMU
MNPESENALTASDDCIGHGIPRNADA
GYNBOTITGSHANGNIGAISHIAWLA
TEOETSRISESAWTNIEFTIHORG TB
TREETRPNVDOIYORCSOEORTNAAS
ELEERKOMVGNMLRYEUARSRNIFR
LTHMTSLWETNAHRNEEAAL EIONDK
ABADLEATNWDBUOETRDHWFYENGB
SPDRUFYEOLAERNOILLOACHAWTW
INEIPNOSDASTSLUINNACKSSDPN
SOOSIITTUUNSF L DAKNHOLNFSCA
DTIGWAARNOIRHTNADDELGALTOS
NEWRSGHIEMNATNAEITNCDWIHED
IHVROOHDEARRIAEMEINTNGCTGN
AETHUOHSTLOKRWUEETNTAOATBB
AAEBHANMRYILBTEYHDCIOPTNTP
ORORPEFXOAMMASTGAHCEE GTPSN
EPYFLWSROMCHAPDUTJSUEAOHIH
ITEOMWELTHCHRURONEESBPTIOS
```

The ciphertext above was obtained from the plaintext by permuting (rearranging) the columns of the array. To decrypt, we need to find the inverse permutation, i.e., to reorder of the columns in the array to get back to the plaintext.

Using the technique discussed in class, we compute the matrix below, in which the entry in row  $i$ , column  $j$  gives us an estimate of the probability that column  $i$  is followed by column  $j$  in the reordering of the columns above that brings us back to the plaintext. (Actually, the table entry is  $\log_{10}(p_{ij})$ , where  $p_{ij}$  is our estimate of the probability.) If column  $i$  the last column in the reordering, then row  $i$  of the matrix is not meaningful.

---

<sup>1</sup> In general, we would not know the degree. But we could try a number of degrees till we came out with a sensible result.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	---	-19.61	-14.18	-14.21	-16.56	-21.19	-16.03	-11.82	-15.67	-14.35	-8.70	-12.23	-23.12	-17.19	-20.43	-11.75	-14.42	-14.63	-11.51	-9.76	-18.33	-13.88	-10.22	-10.24	-12.63	-0.00
1	-18.59	---	-16.77	-15.03	-17.71	-23.65	-13.68	-14.46	-17.45	-14.30	-12.57	-16.46	-0.00	-18.00	-11.04	-13.11	-22.00	-19.80	-15.98	-21.29	-27.85	-19.17	-17.93	-11.88	-22.27	-22.84
2	-21.38	-23.37	---	-21.39	-22.68	-25.12	-24.32	-21.53	-0.00	-25.99	-26.82	-22.07	-21.20	-26.91	-20.73	-23.12	-21.03	-22.73	-32.39	-22.56	-25.52	-21.12	-20.93	-18.44	-25.44	-25.90
3	-16.18	-0.00	-17.01	---	-14.15	-9.88	-18.06	-15.59	-14.62	-16.26	-13.30	-18.53	-16.40	-16.32	-9.95	-16.38	-16.20	-17.86	-15.78	-11.50	-19.99	-14.05	-4.86	-23.25	-13.97	-18.48
4	-15.63	-18.79	-0.00	-13.26	---	-23.01	-16.62	-16.19	-24.85	-15.92	-10.41	-17.59	-16.52	-16.82	-16.40	-16.89	-22.19	-14.06	-15.48	-17.80	-20.87	-21.09	-17.84	-15.54	-13.75	-21.25
5	-13.36	-21.15	-11.73	-6.05	-14.70	---	-14.00	-10.17	-13.41	-16.05	-7.81	-4.38	-13.42	-16.45	-14.43	-11.33	-17.47	-10.80	-10.07	-12.45	-14.25	-13.68	-11.41	-0.00	-10.97	-15.18
6	-16.92	-11.33	-18.82	-16.29	-16.52	-17.13	---	-18.23	-12.89	-16.34	-18.65	-16.05	-16.35	-15.88	-11.11	-10.56	-0.00	-12.72	-15.48	-5.68	-21.07	-21.38	-14.30	-13.97	-15.09	-18.02
7	-17.14	-24.86	-15.12	-21.97	-22.25	-22.98	-22.03	---	-27.16	-12.31	-18.86	-22.78	-20.12	-16.72	-16.71	-18.14	-23.35	-21.61	-0.00	-19.43	-18.43	-21.13	-18.30	-27.38	-18.40	-21.76
8	-14.18	-22.43	-13.90	-0.00	-20.32	-22.36	-19.00	-19.59	---	-21.53	-7.64	-16.24	-23.45	-14.01	-18.59	-14.03	-23.15	-17.00	-15.02	-18.35	-22.41	-21.01	-18.56	-10.26	-15.62	-20.36
9	-8.08	-13.38	-11.01	-5.59	-9.29	-14.44	-11.78	-7.72	-16.08	---	-3.80	-0.00	-13.92	-12.78	-10.74	-4.02	-15.11	-8.63	-13.29	-6.39	-15.86	-12.32	-2.99	-4.65	-7.86	-10.19
10	-0.00	-8.65	-15.34	-14.06	-9.17	-10.92	-3.11	-5.57	-8.38	-4.79	---	-8.15	-9.85	-9.64	-5.67	-6.66	-7.59	-2.53	-5.25	-9.38	-7.04	-7.38	-3.05	-5.18	-7.79	-12.69
11	-0.00	-18.74	-12.81	-16.15	-12.39	-12.62	-13.37	-14.79	-21.12	-17.72	-14.48	---	-16.56	-15.15	-9.93	-18.41	-18.54	-16.32	-11.05	-9.10	-24.58	-16.03	-11.74	-17.60	-15.64	-16.52
12	-21.63	-15.56	-11.30	-10.13	-12.11	-18.24	-17.59	-10.47	-16.35	-15.54	-15.33	-15.94	---	-16.93	-13.43	-0.00	-13.71	-18.82	-15.59	-13.74	-21.01	-23.25	-15.94	-14.50	-15.27	-17.48
13	-4.76	-11.29	-15.95	-11.49	-9.31	-12.10	-9.91	-8.02	-13.07	-12.53	-9.00	-12.40	-11.33	---	-12.03	-1.65	-8.27	-14.08	-14.71	-2.60	-0.01	-9.96	-3.91	-4.96	-13.66	-10.83
14	-11.67	-22.09	-14.90	-11.37	-16.53	-15.49	-17.12	-18.54	-17.14	-14.21	-13.18	-23.09	-21.34	-18.62	---	-14.96	-16.39	-0.00	-13.55	-15.14	-20.37	-16.90	-19.93	-12.34	-12.74	-17.10
15	-14.56	-17.89	-20.02	-12.90	-19.74	-16.59	-18.89	-18.16	-22.54	-20.39	-14.05	-18.18	-15.25	-0.00	-13.92	---	-16.92	-14.38	-19.69	-16.87	-23.65	-18.16	-13.74	-21.60	-16.24	-25.19
16	-19.84	-26.39	-16.03	-15.35	-18.79	-24.54	-16.26	-21.62	-23.76	-23.23	0.00	-18.11	-22.24	-18.15	-21.30	-22.57	---	-19.51	-16.91	-21.21	-27.44	-19.43	-16.37	-20.44	-17.72	-16.95
17	-19.65	-20.33	-22.46	-21.98	-20.77	-16.80	-17.49	-17.85	-20.22	-22.56	-14.18	-22.90	-20.50	-23.82	-18.22	-15.33	-25.08	---	-32.22	-0.00	-20.27	-15.99	-15.60	-14.44	-18.73	-19.15
18	-16.49	-17.01	-22.58	-24.03	-16.75	-0.00	-24.95	-15.78	-17.22	-19.15	-22.18	-22.66	-18.95	-21.19	-13.88	-21.56	-13.63	-23.01	---	-9.24	-21.97	-20.69	-20.22	-15.54	-22.02	-21.44
19	-15.77	-18.33	-13.27	-12.56	-22.52	-19.40	-0.00	-13.55	-21.79	-11.07	-16.43	-20.31	-15.54	-16.09	-13.23	-19.59	-16.79	-16.54	-15.00	---	-24.25	-16.75	-16.45	-14.32	-14.45	-23.29
20	-22.51	-24.69	-21.46	-17.83	-22.72	-28.10	-20.12	0.00	-28.61	-21.30	-25.69	-24.20	-22.35	-19.15	-19.20	-20.72	-22.12	-17.99	-22.89	-21.19	---	-26.78	-21.12	-19.36	-22.26	-24.78
21	-17.25	-28.82	-16.17	-20.07	-20.86	-26.32	-21.58	-14.79	-26.30	-24.93	-12.77	-25.67	-24.14	-15.90	-0.00	-26.83	-26.80	-25.95	-21.25	-21.46	-34.38	---	-16.84	-22.59	-22.13	-25.87
22	-16.07	-25.52	-17.97	-15.05	-21.22	-18.25	-14.32	-23.31	-18.12	-0.00	-18.43	-22.31	-16.93	-19.75	-18.28	-15.10	-15.42	-17.13	-16.37	-18.02	-26.25	-23.03	---	-12.21	-11.38	-25.44
23	-18.91	-10.60	-19.65	-20.83	-18.26	-20.63	-19.16	-17.36	-24.85	-21.91	-17.97	-19.99	-14.56	-24.37	-16.83	-20.24	-22.99	-24.70	-19.81	-15.35	-22.67	-17.20	-0.00	---	-16.41	-25.44
24	-12.98	-17.68	-19.39	-17.22	-0.00	-15.64	-13.09	-10.58	-19.94	-18.06	-14.54	-18.97	-14.03	-24.16	-10.41	-11.90	-11.22	-23.79	-16.89	-10.68	-20.27	-13.63	-14.40	-18.07	---	-17.87
25	-16.03	-21.95	-24.58	-27.59	-26.99	-24.39	-17.98	-24.34	-28.58	-18.18	-26.40	-30.00	-19.07	-26.27	-20.09	-24.43	-17.50	-25.53	-27.22	-22.79	-25.31	0.00	-17.08	-27.11	-21.03	---

The first column after reordering is presumably column 24, since no other column is likely to be followed by column 24. The reordering of the columns that gives the plaintext is, in all likelihood:

**24 4 2 8 3 1 12 15 13 20 7 18 5 23 22 9 11 0 25 21 14 17 19 6 16 10**