Bevezetés a számításelméletbe II.

2005. MÁJUS 19.

14. gyakorlat: Kódolás

Sikerült elfognunk Recski tanár úr e-mailjét, amit Szeszlér tanár úrnak küldött, és leírja benne, hogy mi lesz a kérdés a vizsgán. Sajnálatos módon a levél az RSA algoritmussal titkosítva van, de az ismeretes, hogy Szeszlér tanár úr nyilvános kulcsa (85,43). Az eredeti üzenetben a számok jelentése:

A=2	D=6	G=11	J=21	M=26	P=31	S=36	V=41	Y=46
B=3	E=7	H=12	K=22	N=27	Q=32	T=37	W=42	Z=47
C=4	F=8	I=13	L=23	O=28	R=33	U=38	X=43	=48

A titkosított üzenetben a következő számok szerepelnek: 8, 27, 58, 48, 22, 81, 48, 76, 27, 8, 3, 6, 8, 46. Próbáljuk meg dekódolni a levelet!