دانشکده علوم ریاضی و آمار

مدرس: **دکتر مجتبی رفیعی** نیمسال دوم ۱۴۰۰-۱۴۰۱

آزمایشگاه رمزنگاری - تمرین سری اول

زمان اشتراک گذاری: ۲۴ *فروردین* ۱۴۰۱ ***مهلت تحویل:*** ۱۰ *اردیبهشت* ۱۴۰۱

شکستن سیستم‌های رمزنگاری کلاسیک

(۱۰۰ نمره) به منظور آشنایی بیشتر با مفاهیم تدریس شده در کلاس برای رمزنگاری کلاسیک، تمرین پیش رو معرفی شده است. فهرست زیر نشان می‌دهد که هر مساله مربوط به کدام دانشجوست.

شماره دانشجویی	شماره مساله	شماره دانشجویی	شماره مساله
۹۷۱۸۱۳۰۱۰	۱	۹۷۱۸۱۳۱۸۱	۱۵
۹۵۱۸۱۱۱۹۳۰۰۲	۲	۹۷۱۸۱۳۱۸۴	۱۶
۹۷۱۸۱۳۰۲۵	۳	۹۷۱۸۱۳۱۸۹	۱۷
۹۷۱۸۱۳۰۴۰	۴	۹۷۱۸۱۳۱۹۰	۱۸
۹۷۱۸۱۳۰۵۰	۵	۹۶۱۸۱۳۲۶۲	۱۹
۹۸۱۸۵۳۰۰۳	۶	۹۷۱۸۱۳۲۶۱	۲۰
۹۶۱۸۱۳۱۳۰	۷	۹۷۱۸۶۳۰۵۶	۲۱
۹۷۶۰۰۳۱۱۶	۸	۹۷۱۸۱۳۳۰۰	۲۲
۹۷۱۸۱۳۱۲۸	۹	۹۷۱۸۲۳۰۱۷	۲۳
۹۵۱۸۱۱۱۹۳۰۱۷	۱۰	۹۷۱۸۱۳۳۱۷	۲۴
۹۷۱۸۵۳۰۰۵	۱۱	۹۷۱۸۱۳۳۳۴	۲۵
۹۷۱۸۱۳۱۶۴	۱۲	۴۰۰۴۰۱۴۰۰۲	۲۶
۹۷۱۸۱۳۱۶۵	۱۳	۹۹۴۰۳۴۰۰۲	۲۷
۹۷۱۸۱۳۱۷۴	۱۴	۴۰۰۴۰۱۴۰۴۰	۲۸

برای هر یک از دانشجویان عزیز، یک فایل مربوط به فرکانس‌های تکرار دو حرفی مربوط به متن اصلی‌شان در صورت سوال به صورت اختصاصی ارایه شده است. در ادامه یک مثال برای نحوه محاسبه فرکانس‌های مذکور آورده شده است. فرض کنید متن آشکار ما abcabab باشد، در اینصورت فرکانس تکرار دو حرفی ab برابر $\frac{1}{6}$ می‌باشد.

جدول زیر یک نمونه از فایل تست ایجاد شده درکویرا را نشان می‌دهد. همانطورکه در جدول مشخص است، ستون سمت چپ حاوی متن رمزی و به عنوان ورودی برنامه است و ستون سمت راست خروجی مورد انتظار با قالب زیر است:

- سطر اول حاوی یک عدد صحیح به عنوان طول کلید است،
- سطرهای بعدی حاوی متن اصلی است که به صورت کاراکترهای متوالی و بدون فاصله‌گذاری می‌باشد.

نکته: در صورت نیاز به دنباله‌زنی، از کاراکتر خط فاصله/تیره (یعنی -) استفاده شده است.

Input (Ciphertext)	Output (Plaintext)
aoanthaoaasiopticiameluihnreepuvrcmasrs asualnolsnooaehsapieeeadreentaoxrrpfiimi tibaeToaefeedtooeosrvoahnpnnnnsegueeld eeutslBlaslioorrnklgledghhdtardtsegotpnn navethldfimaaabbsnrhradeoredtatmedoota tacdhlsahhamodasfyhneyhnadmlswahdsler etiaahoylpsdcfemridabiennlstdteiloroleoue calschiltotertcdhgcnanttiehaosihinlliaboyu oirhlgaaqdaauaodaastielFehhaatniiebtusns omdtdolnrntamlpinlnciltaeedtedrneetmcai McernpaseItokltewsrpcIwnaoslditrtdylatni ohcanahdslomrdidbnwesittegodeugietntici snrhcdrykclsnrnegsabsruwaehscehshdonfl ddkredhetepoatlriyttiiigerratssnheItsnhshd fAeiodeareflnprtedntecgheliamebotaslhnlu anmshhseisyaniyiexasedetrgdivttavntderde eeophrhdshkieracttusnioyapnofoyendorita oiilobrubbrnnduiyohndoureystidosiehddgp dIobaatepmdethoiseseeilqtfaavnaoodeoerf deroeeipbyigofhcalecbsvmetiiarcfeoasolsa tatesheoekehhnotyitdertnnieaeyiefnhyrueh ddgrosdegoetfagiopnapdnctoieiaiendccrau igeprtaiorsnnmmdeeute	5 Iamagooddebaterandoratorathleteandsport smanandatthesametimeIholdtoppositionsin theclassintheacademicfieldAllthequalitieso fheadandhearthaveearnedmeaprofoundlov eandrespectfrommyteachersandfriendsMy teachersencourageandhelpmeinallpossible waysIaminthegoodbooksofalltheteachersa swellastheprincipalbecauseIhavewonmany medalstrophiesshieldsandcertificatesformy extraordinarydisplayofabilitiesinexaminati onsathleticsdebatesandtheatreThegoodidea slikeloveforthemotherlanddevotiontodutyo bediencetowardseldersservicetothenationh elpingthepoorandtheneedynursingthesickf eedingthehungryetcareinculcatedinthestud entsduringtheirschooldaysBroadlyspeakin gschoollifeisnotonlyforlearningreadingboo ksorplayingbutalsoaperiodduringwhichallt hegoodhabitsareacquiredbadhabitsareshun nedandgoodconductfairplayandsoundthink ingaredevelopedFurtherthehealthyideasofp atriotismandnationalismareimbibedbythest udentsduringthisperiod

متن اصلی مثال بالا با فاصله گذاری به صورت زیر است:

I am a good debater and orator, athlete, and sportsman and at the same time, I hold top positions in the class in the academic field. All the qualities of head and heart have earned me a profound love and respect from my teachers and friends. My teachers encourage and help me in all possible ways. I am in the good books of all the teachers as well as the principal because I have won many medals, trophies, shields, and certificates for my extraordinary display of abilities in examinations, athletics, debates, and theatre.The good ideas-like love for the motherland, devotion to duty, obedience- towards elders, service to the nation, helping the poor and the needy, nursing the sick, feeding the hungry, etc – are inculcated in the students during their school days.Broadly speaking, school life is not only for learning, reading books or playing, but also a period during which all the good habits are acquired, bad habits are shunned and good conduct, fair play, and sound thinking are developed. Further, the healthy ideas of patriotism and nationalism are imbibed by the students during this period.

فرکانس تکرار حروف دوتایی در متن آشکار:

دو حرفی	تکرار	دو حرفی	تکرار
hi	۰/۰۰۴۵۱۶۷۱۲	er	۰/۰۰۹۹۳۶۷۶۶
de	۰/۰۰۹۰۳۳۴۲۴	an	۰/۰۱۴۴۵۳۴۷۸
nt	۰/۰۰۱۸۰۶۶۸۴۸	es	۰/۰۰۵۴۲۰۰۵۴۳
sa	۹/۰۳۳۴۲۴$E-۴$	et	۰/۰۰۲۷۱۰۰۲۷۲
se	۰/۰۰۱۸۰۶۶۸۴۸	ve	۰/۰۰۴۵۱۶۷۱۲
si	۰/۰۰۳۶۱۳۳۶۹۵	ra	۰/۰۰۲۷۱۰۰۲۷۲
of	۰/۰۰۴۵۱۶۷۱۲	te	۰/۰۰۷۲۲۶۷۳۹
ea	۰/۰۱۱۷۴۳۴۵۱	ar	۰/۰۰۹۰۳۳۴۲۴
ur	۰/۰۰۵۴۲۰۰۵۴۳	re	۰/۰۰۸۱۳۰۰۸۱
on	۰/۰۰۷۲۲۶۷۳۹	at	۰/۰۱۱۷۴۳۴۵۱
ed	۰/۰۰۹۰۳۳۴۲۴	th	۰/۰۲۳۴۸۶۹۰۱
st	۰/۰۰۱۸۰۶۶۸۴۸	nd	۰/۰۱۶۲۶۰۱۶۲
or	۰/۰۰۸۱۳۰۰۸۱	ld	۰/۰۰۳۶۱۳۳۶۹۵
in	۰/۰۱۹۸۷۳۵۳۲	ha	۰/۰۰۳۶۱۳۳۶۹۵
ou	۰/۰۰۲۷۱۰۰۲۷۲	ng	۰/۰۱۰۸۴۰۱۰۹
en	۰/۰۰۴۵۱۶۷۱۲	le	۰/۰۰۳۶۱۳۳۶۹۵
is	۰/۰۰۴۵۱۶۷۱۲	to	۰/۰۰۴۵۱۶۷۱۲
it	۰/۰۰۴۵۱۶۷۱۲	he	۰/۰۲۷۱۰۰۲۷
al	۰/۰۰۸۱۳۰۰۸۱		