**Program Studi Teknik Informatika**

**Sekolah Teknik Elektro dan Informatika**

**Institut Teknologi Bandung**

**===============================**

# **Tugas 2 IF4020 Kriptografi**

# **Semester II Tahun 2023 / 2024**

Batas pengumpulan : Senin, 26 Februari 2024, 20:40 WIB

Tempat pengumpulan : <https://forms.gle/RYKfZixVTNHdA8jQ8>

Berkas pengumpulan : File format PDF

Anggota kelompok : 2 orang (disarankan sama dengan tugas 1)

Yang dikumpulkan adalah: laporan sederhana yang berisi

a. Berkas cipherteks

b. Langkah-langkah yang anda lakukan dalam melakukan dekripsi

c. Plainteks hasil dekripsi

Informasi Tambahan:

Pada proses pembuatan ciphertext, plainteks diubah seluruhnya menjadi kapital. Lalu, enkripsi hanya dilakukan pada karakter abjad (A..Z). Karakter lain (angka, spasi, koma, titik, dan lain-lain) dibuang (tidak dienkripsi).

## **Kriptanalisis pada Cipher Abjad-Tunggal**

Conan bersama teman-temannya, menemukan sebuah dokumen mencurigakan di tempat kejadian perkara. Mereka tertarik sebab dokumen tersebut berada dalam bentuk terenkripsi. Conan dan kawan-kawan mencoba memecahkan cipherteks tersebut. Informasi tambahan yang telah diketahui adalah dokumen tersebut aslinya dalam bahasa inggris lalu dienkripsi dengan ***cipher* substitusi abjad-tunggal** *(monoalpahtbetic cipher)*.



Bantulah Conan untuk dekripsi chiperteks tersebut menjadi plainteks semula meskipun anda tidak mengetahui kuncinya. Anda dapat menggunakan kombinasi teknik analisis frekuensi dan metode terkaan untuk mendekripsi dokumen tersebut. Anda diperbolehkan menggunakan kakas bantu (coretan kertas, aplikasi Ms Excel, kakas bantu, maupun membuat program kecil sederhana untuk menghitung frekuensi kemunculan karakter atau untuk keperluan analisis lainnya) untuk menyelesaikan masalah ini. Carilah data tabel frekuensi kemunculan huruf, bigram, dan trigram dalam Bahasa Indonesia untuk membantu kriptanalisis.

XBMVHRWROMLAHZEAHUCMRGAEXBEHXRCEALFAVEYILFORGXBMVHRWROMTECLAXUAAHTRPYLFKBYFXZEAXBMVHROBYVZMLAXRFXEBFECTLHZHZETBLHLFORGPEAAYOEALFAEXBEHXRCEYFCHZEXBEYHLRFRGHZEAEPEHZRCATZLWEXBMVHYFYWMALALAXRFXEBFECTLHZBEYCLFOEFXBMVHECPEAAYOEAKMKBEYILFOAEXBEHXRCEAYFXLEFHHLPEAAYTPYFMEDYPVWEARGXBMVHROBYVZMRNEBHZBEEHZRUAYFCMEYBAYOREOMVHLYFAXBLKEAPYCEUAERGZLEBROWMVZLXHBYFAGRBPYHLRFAHRRKAXUBEHZEPEYFLFORGTBLHHEFPEAAYOEAPEARVRHYPLYFYFCKYKMWRFLYFAXBLKEAEPVWRMECALPLWYBHEXZFLQUEAHRBEFCEBXUFELGRBPHYKWEHAUFBEYCYKWEHRHZEUFLFLHLYHECHZEOBEEIAEPVWRMECXBMVHROBYVZMYFCHZEXWRAEWMBEWYHECAHEOYFROBYVZMTZLXZLAXRFXEBFECTLHZXRFXEYWLFOHZEEDLAHEFXERGXRPPUFLXYHLRFBYHZEBHZYFXRFHEFHGRBPLWLHYBMYFCHYXHLXYWVUBVRAEAENEFHZEIYPYAUHBYRGYFXLEFHLFCLYHRUXZEARFXBMVHROBYVZMWLAHLFOAEXBEHTBLHLFOYARFERGHZEALDHMGRUBGUFCYPEFHYWYBHAZUFCBECARGRHZEBEDYPVWEARXXUBLFYFXLEFHXLNLWLSYHLRFALFAZRBHXBMVHROBYVZMZYAYVVEYBECPRBERBWEAAAVRFHYFERUAWMLFENEBMXUWHUBELFTZLXZWLHEBYXMZYAKEXRPETLCEAVBEYCXBMVHYFYWMALARFHZERHZEBZYFCHRRIXRFALCEBYKWMWRFOEBHRCENEWRVYAYBLORBRUAAUKJEXHRGAHUCMHZEEYBWLEAHAUBNLNLFOCEAXBLVHLRFARGAMAHEPYHLXPEHZRCARGXRCEKBEYILFOXRPEGBRPGLGHEEFHZXEFHUBMLFHZEYBYKLXEFXMXWRVECLYAUKZYWYAZYLHOLNEAHZEGLBAHIFRTFTBLHHEFCEAXBLVHLRFRGHZEHEXZFLQUERGGBEQUEFXMYFYWMALATZEBEHZEGBEQUEFXLEARGWEHHEBAYFCWEHHEBOBRUVLFOARGYWYFOUYOEYBEUAECHRUFBYNEWAEXBEHXRCEAXBMVHRWROMZYAVWYMECYBRWELFVRWLHLXYWYFCPLWLHYBMPYHHEBAGBRPPECLENYWHLPEAHZBRUOZHZEXEFHUBMVEBZYVAPRAHGYPRUALAHZEXBMVHRWROLXEGGRBHRGOBEYHKBLHYLFYFCHZEUFLHECAHYHEACUBLFOTRBWCTYBLLHZEEGGRBHARGHZLBHMHZRUAYFCEPVWRMEEAYHKBLHYLFAKWEHXZWEMVYBILFXBMVHYFYWMSLFOOEBPYFMAEFLOPYHBYFAPLAALRFALAAYLCHRZYNEAZRBHEFECHZETYBKMAENEBYWMEYBAYFCLHWECHRHZECENEWRVPEFHRGHZEGLBAHCLOLHYWXRPVUHEBXRWRAAUAALPLWYBEGGRBHALFHZEUFLHECAHYHEAHRKBEYIJYVYFEAEXRCEAYLCECYPEBLXYFLFHEWWLOEFXELFHZETYBXRFNLFXLFOYPEBLXYFYUHZRBLHLEARGHZELPVRBHYFXERGXBMVHRWROLXEDVEBHLAEYFCENEFHUYWWMWEYCLFOHRHZEEAHYKWLAZPEFHRGHZEFYHLRFYWAEXUBLHMYOEFXMLFTLHZHZEBLAERGCLOLHYWXRPVUHEBFEHTRBIALFHZEAEXUBLFOXRPPUFLXYHLRFKEXYPEYFLFXBEYALFOWMLPVRBHYFHHYAILFHZEVBLNYHEAEXHRBYATEWWHZEFEECARGHZEKYFILFOLFCUAHBMLFVYBHLXUWYBGRBAEXUBECLOLHYWXRPPUFLXYHLRFKEXYPEEAVEXLYWWMUBOEFHCENEWRVPEFHAYHLKPWECHRHZECEALOFRGWUXLGEBRFERGHZEGLBAHVUKWLXXLVZEBAGRBXRPVUHEBXRPPUFLXYHLRFAHZEFYHLRFYWAEXUBLHMYOEFXMRGGEBECAENEBYWLPVBRNEPEFHAHRWUXLGEBYFCLFHZEFYHLRFYWKUBEYURGAHYFCYBCAVBEAEFHECHZEPRCLGLECNEBALRFYAHZECYHYEFXBMVHLRFAHYFCYBCRBCEAHZUAHZEGLBAHVUKWLXAHYFCYBCGRBEFXBMVHLRFKEOYFHROYLFTLCEAVBEYCUAEYPEHZRCRGAEXUBLFOXRPPUFLXYHLRFLAXYWWECYXBMVHRAMAHEPHZEAEFCEBEFXBMVHARBEFXLVZEBAYPEAAYOEUALFOYFEFXBMVHLRFYWORBLHZPHROEHZEBTLHZYAEXBEHIEMHZLAVBRCUXEAYXLVZEBHEDHTZLXZLAAEFHHRHZEBEXLVLEFHHZEBEXLVLEFHTZRYWARVRAAEAAEAYIEMBEXELNEAHZEXLVZEBHEDHYFCCEXBMVHARBCEXLVZEBAUALFOHZEIEMHRBEXRNEBHZERBLOLFYWPEAAYOEXYWWECHZEVWYLFHEDHLFHZEZLAHRBMRGXBMVHRWROMUVHRYWWXBMVHRAMAHEPABEQULBECHZEAEFCEBYFCHZEBEXELNEBHRYOBEEKEGRBEZYFCRFHZEAYPEIEMYIEMHZYHZYCHRKEBLORBRUAWMVBRHEXHECGBRPEDVRAUBEHRYFYCNEBAYBMHZLALAIFRTFYAAMPPEHBLXRBAEXBEHIEMXBMVHROBYVZMYBBYFOLFOHRAZYBEYAEXBEHIEMKEHTEEFHTRVYBHLEALARGHEFYCLGGLXUWHVBRKWEPYFCCREAFRHAXYWETEWWHRAXEFYBLRALFTZLXZPYFMLFCLNLCUYWARBXRPVUHEBAPLOZHXRPPUFLXYHETLHZEYXZRHZEBLFPYBHLFZEWWPYFYVBRGEAARBYHAHYFGRBCUFLNEBALHMYFCTZLHGLEWCCLGGLEYOBYCUYHEAHUCEFHLFHBRCUXECHZEXRFXEVHRGYAMPPEHBLXRBVUKWLXIEMXBMVHROBYVZMLFHZELBAEPLFYWVYVEBFETCLBEXHLRFALFXBMVHROBYVZMHZEMAVEXUWYHECHZYHYPEHZRCRGEFXBMVHLRFPLOZHEDLAHLFTZEBEHZEEFXBMVHLRFIEMCLGGEBECGBRPHZECEXBMVHLRFIEMLFAUXZYAXZEPEYUAEBAEFXBMVHLRFIEMXRUWCKEYFFRUFXECHRHZEVUKWLXYFMRUHALCEBXRUWCRKHYLFHZLAVUKWLXEFXBMVHLRFIEMYFCUAELHHRAEFCEFXBMVHECPEAAYOEAHRHZEUAEBALFXERFWMHZEUAEBTRUWCVRAAEAHZECEXBMVHLRFIEMRFWMAZEXRUWCRKHYLFHZECEXBMVHLRFRGHZEPEAAYOEVUKWLXIEMXBMVHROBYVZMYWARRVEFECCRRBAGRBPYFMRHZEBYVVWLXYHLRFAAUXZYACLOLHYWALOFYHUBEAYFCEWEXHBRFLXXYAZHZEXRFXEVHRGVUKWLXIEMXBMVHROBYVZMXLBXUWYHECLFHZEBEAEYBXZXRPPUFLHMGRBARPEHLPEKEGRBEHZEGLBAHVBYXHLXYWVBRVRAYWGRBAUXZYAXZEPETYAPYCELFYUOUAHHZEBAYVUKWLXIEMXBMVHRAMAHEPFYPECYGHEBLFNEFHRBABRFBLNEAHYCLAZYPLBYFCWEFYCWEPYFTYALFHBRCUXECLFPYBHLFOYBCFEBAXRWUPFRFPYHZEPYHLXYWOYPEALFAXLEFHLGLXYPEBLXYFHZEBAYXBMVHRAMAHEPRUHWLFECLFAEXHLRFZYAAUBNLNECRNEBHTEFHMMEYBARGAHUCMKMXBMVHYFYWMAHALFHZEVUKWLXAEXHRBYFCLHLAHZEPRAHTLCEWMUAECVUKWLXIEMXBMVHRAMAHEPLFHZETRBWCLHLAUAECYPRFORHZEBVWYXEALFHZEAEHVBRHRXRWGRBAEXUBEXBECLHXYBCHBYFAYXHLRFAYFCHZEAAWVBRHRXRWGRBAEXUBEXRPPUFLXYHLRFRFHZELFHEBFEHVUKWLXCLAXUAALRFYFCBEAEYBXZLFXBMVHROBYVZMLFKUALFEAAYFCYXYCEPLYAHYBHECLFHZEWYAHQUYBHEBRGHZE20HZXEFHUBMYFCXRFHLFUEAYHYGUBLRUABYHEFETPEHZRCAGRBEFXBMVHLRFYBEVUKWLXWMYFFRUFXECBEAEYBXZEBAHZEFAHUCMHZEAEPEHZRCAGRBTEYIFEAAEAKMYVVWMLFOHZEHRRWARGXBMVHYFYWMALA2RFWMYGHEBLFHEFAEVUKWLXAXBUHLFMCREAYFETXBMVHRAMAHEPOYLFYAEFAERGWEOLHLPYXMAHUCMLFOYFCUALFOPEHZRCAGRBKBEYILFOXBMVHRAMAHEPALAYFEAAEFHLYWAHEVLFHZECENEWRVPEFHRGFETCEALOFAGRBPRBEAEXUBEXBMVHRAMAHEPAKMWEYBFLFOZRTHZLFOAKBEYITEWEYBFZRTHRPYIEHZEPAHBRFOEBLHLALFHZLAAVLBLHHZYHHZLAHZEALALATBLHHEFHZLATRBIUAEAPYHZEPYHLXYWHRRWAHRAHUCMHZEBAYVUKWLXIEMXBMVHRAMAHEPYFCAENEBYWNYBLYFHATEUAEHRRWAGBRPFUPEBLXYWYWOEKBYYFCHZEOERPEHBMRGFUPKEBAHROEHRUBBEAUWHAYWOEKBYLXXBMVHYFYWMALAZYAVBRNEFHRKERFERGHZEPRAHEGGEXHLNEPEHZRCALFHZEAHUCMRGVUKWLXIEMXBMVHRAMAHEPA

Setelah menemukan plainteksnya, carilah di Google teks tersebut berada untuk mendapatkan tanda baca di dalam teks aslinya.

## Metode Kasiski



Kalian mendapatkan tugas penting dari detektif Kogoro Mouri, yaitu memecahkan sebuah dokumen berisi cipherteks. Dokumen tersebut berisikan sejarah tersembunyi sebuah bangunan antik yang sudah dienkripsi. Conan, yang sudah mengambil mata kuliah IF4020 Kriptografi, ingin membantu kalian memecahkan dokumen tersebut. Akan tetapi, dia dimarahi oleh Ran Mouri karena kalian perlu memecahkannya sendiri demi mendapatkan nilai pada tugas kali ini. Conan yang baik kemudian memberitahu kalian sebuah *hint*, bahwa dokumen tersebut dienkripsi dengan **Vigenere Cipher** dan ditulis menggunakan **bahasa Inggris**. Yuk pecahkan bersama Conan! Temukan terlebih dahulu kunci yang digunakan untuk mengenkripsi dengan metode **Kasiski**.



Setelah menemukan kuncinya, dekripsilah cipherteks di atas dengan menggunakan program Vigenere cipher standard yang telah kalian buat pada tugas 1. Editlah hasil dekripsi tersebut sehingga enak dibaca, tambahkan tanda baca yang relevan jika perlu (karena program Vigenere Cipher yang digunakan mengabaikan tanda baca).

## Kriptanalisis *Playfair Cipher*



Ai Haibara kehilangan sebuah bagian dari novel. Rupa-rupanya, bagian novel tersebut telah dicuri oleh Profesor Hiroshi Agasa dan digunakan untuk sebuah eksperimen. Ternyata, eksperimen tersebut gagal dan justru membuat bagian novel Ai menjadi aneh. Conan yang mencintai Kriptografi kemudian menyadari bahwa novel **berbahasa Inggris** tersebut telah dienkripsi menggunakan **Playfair Cipher**. Bantulah Conan untuk mendekrip bagian novel tersebut demi Ai! Gunakanlah analisis frekuensi kemunculan bigram dalam bahasa Inggris.

PMEXMNMVOQMVALUKXFQPNTPWPOMSSYMTECSYMTNHMHSMPOCEGPHIHETHHEHQNHMHMLPWTDHAQWKPSEAHETWDUKZPHMQRZOEHELKHHMLHELATVAMLPFALUKQOANMLVZLCNTQXPCTPQMQXEXZHAYXDVASHXDLDMPIRHLSYPOVXTDLIMAHEHQZIVAGQMEHEPUKNZAARZOEWDFMAXMQNMKYPPAHQXHVAELGQMHVZKPPLLXYSVDTAALOCPYFBXQXDRXAYKTSEMQKMUAAPELXHXIXZCXANLNQREXXYHEETMKHUEXQWTDGHAHLKIOAWELGQKETSLTMTWKATSKQNPOVATGELPMMGYPPAHQXHVAAYXEEMFTDFMQEXKEEGEQHSHUHBZGLHELIPILATPDQFLCXFTDRHAYKTGTNQQXMTWKIPLNOUIXRAAMMLBEPGPQKTPLELVHQSTDSHXQXDCPHMSIMKQENLBDAMVSQZXDDFHEQEAQKAFCYPVAELOQMVALIRETGEVPTAAPDFGTAFALGNOQOEHQEXGQBEELYSPFQXUGBEELMHXHMXPLQXHMFCIHWQHYHMLHELOQMVALIRETMQMTWKHEQXCAELKHEXHLCNZLHEHQTAPGETGEMAKVLHEXCEELYSKSLTHLVANLHSXHVAETAVDPTNGOKHPOEOGQVGCPHMZAHEHQGQMEABHEQXCHELZKPOEONTHSZAUXEXUKEQLPQFOGZLTXPOABHELMCLHLMVPMVSCLHLWHIXPMMGYPPAHQXAXGVAHMFZABHEHQETMEEVLHLPMVTMHMTAQHHSXGFXTGEVMVOQMVALURMHHLEMQMRAQMQGBEETMTIXGXHLVWTDLIMAELMVGXHLSHEMELSKGFGOLPMWCLAYXDLYVXEXKNHMLTPIEMYPPAHQGXETXGHBIXFPXAXGFTLHCFLHELOQMVALIRRAQOMQMHCECLAYWDHYTHHEQEAQKAFCYPRXPOEOXIQZBLELFPABHLMVHSSYMTGQBEELVAMHLHHEQMYPPAHQRGEQBHETABHELMCLHLMVETGEVPTAAPDFLCCFZLHEHQETMETMHMTMQEMAQEAYVEAYVXKUXHXIFDHEHMCGGOMHIXDFLPWRANLMQXCAELFPABHLMVHXHIHEHQGQMEHBEXECQOALQRGAQXKXZAETKTUAOEYGLHETHBELENSHEMPMMGYPPAHQFKDHOFDFHEQMOUAOMHZHQLMGHIPOMVLCWKVAHSAVHEHMHNIXFDHEQXSIFCZLHETDUPQOIRRKPOAVQGLHGPIODAVAHETHVASHXDLTEMRQVAHMUGIPHEQXSXFKOUGMGFDFNTETSFMLXQXDTAUPMTVHELKGQFHVQRMKYPPAHQLYSNNQGERALMZGDHOGZLAYVPGPZTKPQXCAQALPWHKPGHEMPMMGYPPAHQCGXAXGMLGEXHKYLSSUHUIXRAHNMHVAALGEVGMHESQXCOQOALQZBEKLGXAYKAKTIGMWDFLDBLELNECLZGQMTAHSDAHTNFUKFHLUZLHLMSIXABHEHNQXOGXHHETALFIXHLGSEHPMOQMVALURZGDHOQRLGXWVQABOIXLMTDDHMNMVOQMVALUKBEELKTANHDEXCESYQMLCGYXAMGQOALIKGFGOWZTNZLSQXAMACNTDLIMAOQOEHQXHMXKFETSZXDTHEXHVQPEXCEYWKFQXKAGXDTMHTATHHEHNTAAPAUABHALHKRTDLKVHALMNMKYPPAHQIXELALBLHELEPOMAELCGAZBEKLGXGTSHEMXTKDQMPOLCXFQPNTPWPOMVKMZSAQHBIXDFHETDKPEQPKBLELVAMHLHHETHELFDAZDTCEELXUMVAVGSFDXPDPLHAYXDMLOZAUHSTGTHMHEGQXSISEFLKPIXTDDFMNMKYPPAHQGQMEHVLTAUMAHYTHELETGMANQEHEQEELQAWRQMAYRALTGEPKQFCEPUGFGDISIGBEELMHXHXIHTWBWZGTAVHTEMQXCGBEELKGMWHMPLSMZSLHKMZSTNZLHEHMHNIXBEESLSQXXGKAHBETZVPOEOELETMTNTQEHEQXGYXDPLZAPQVAETMTNTQETHSYKDPLHELAGSEHPMOQMVALZWAUWDQMEXGMHTMHGEABHETDTHZAVAHSQMXTKDIXPMOQMVALQKPKMTHSPOEMHETDKPEQSHEMOFHEHMGLKEHNTHKTQMHETDTHQXAYVPYSPKSYHBIXFDHWLTGQXDHEAMGSBEETAVIGOMSYMTECSYMTFDUPGDQXSIABHEAMGSBDTHVGPOEOBEMHEGSESVKPXGDXVPMKYPPAHQSIMTAYPVLAXLAUABHAAMETDHEXOMZLHETDTHPOLCWLGXSQEMIXELKMCPLHKFHSGMLCNFELHEPOKALCXFCLAYXDANDTVLTAHSDAKPMQPKNOSYAFAPELXHRAPFQXCAGCLHHETHGEZWZLDFHEANQMDAPLLCNFKMUAAPNHMHKMZSQEPOLCWLGXSQEMWZPGNQHEQXDAAPLTRAAMTHQXHELQPITAPDMWQXCASHXBXUGZESELKGOUMEHELAMFCLZGQXCAETABHEHMAMANQNQMLCNTTACLPLVASHXDLAQKMHXAMAOMLDFULTFCZLMLPFALQXOTGLGRPMOQMVALZKPOEOBENTHSMLPFALHYGOMHXAMAGQFXQFWQOTCLELVAELDALZSVUKIPHXDFUKQFOSLDFULEAMOFFPMACEAYRXIXPGNQVAOFQGEQNXIXAYDFELKMQPNQKEGXXUXDHMPGBEELVAANHMQXKXELLAEXKEGXHQAMNLAFUPXELYGNOELDBLELMANHYSOGXAVAEXGQXDUIZATDUPMAWZHEHQNHMHHYGXMLSYXDANGZHLOEZHGCLHELMPMKYPPAHQXHMAWMISQMLCMALHETHTKGOFALPLHEQNNHMHBEUKQFSIHTAFHFYKHETHSEWEEGLCNTPUMQVHETWEHNIXEXKNLTSYXDEXQNHMTAOCMHQEOTGLCHELEQMRLDWLQSFZABHEQEZAVAPYKDPMOQMVALZHETABHEGXXHVSPKXTFTIRDPAMUAHUVAQFABHEAMLMLDFUHNHMLDTBUGIPHUKGAFALVZQXOXKPPGNQHEQXKIAMHETHFKOUCNAQABHELHSHXBXUDVCPQMDFEXGENLNRQXZLAMATHLMPMKYPPAHQHSSYMTGQBEELKSQFXQXDVGHSSLWRAYVPQXCNTGDGEMSYAFAPPMOQMVALIHHFHIXAXIHBZAAWAYVXTGCHCLELXYEMKFQXAYPGXBXUDTDFHEQEQXHELUGFKPUXELETMEHEQNGSEHETMTLPQFGQHEHSMQVHGKDFDTBESHHLDFKMUAAPHETHPDMWQXKAQMQGBEMALHELKFAPRXGFPFQXOSIXAZFWPKEGGEUHGSEHHEPOKAMLPFALOGNFQXHEAMHVANLHGQCEELURGUBEQMEXOCTIQMPFQEPDZLELGEPGFHLXHLPKFHVSQMCPHMELEGPDVAPLHEQNETMETMHMMAQEEXKFALMTXEEBGSEHAZNQPMOQMVALKYKFTMHMETGEMLPWTDHAQWKPSEUPFHWPANQNKPXQXDELQHAFALGELBZSQMUXNLMHBEMLPFALELSEMQMAMTSHAUPSKPHTBEHLALRLDFTDTAAPEXGMLKZLQMTXZAPDMHELXHXGXEMTWKCGGOPDGOQFAZAFUOBDEHQSHNELWELHLKIOEHELGMHVLHKTAYPAADXIEMXHHOTGPKXAVAELPKEGLCFZKYQSMAULTXQFWPDPHETNHGHMPGSFFPXGHLELONKPCGABHLXEAFATFCZLHELMLDFUAQBDUPHGPIBEUAELSLXAMAGEKSPOFPBLELNEANABLCHETNHGHMRAANHQQMHEQNEXKSUAIHRALMIXMAKEQMQGBEDWKFHYZWZLHEHQSEMQAYPQEQIXZHAYPACLNHMHHYGXMLSYXDANGZHLOEZHGFGLEMELKGOUMEAVANLTXGXDALKGAFALVZQXCAQXZAXHPGWEGXXHZWTGORIXABHEQNOTZLKTQXSIATSKQMPOKAFQAZXEXTCAETHETDLIKAHTNLNBFKMKPGXNETABHEHQNHMHXIQZXDHELMCLHLMVHETHVMGSEHHETHRXETAZELHSKQAMHEAQMVDFETSWWKPMOQMVALIRLCSFMLGNMQEGNLHSLUGFGOQMAYRELAGFGDQMXTKDTHHEHNAYVSHMHMXIXGWLHNEXHLCEGPHIPGNQHEQXCACLELVNZLHEPOKAZTLHHLPKXUHEQMIXELCNTGGHKVGPVAELPKEGLYSWSYQMOFLCAYPGXBXUDTMXLSMLGEHEGXMAKVLHHSQWCLLCGQVAYPWTQSMAZYQMAYVALALMLKEQEXKEEGTAPDVAXUXQRAQMGQTAAUXDAYRADPQEQPNTWHELWETDETXDQMAYVPQXKELMZLHEHMTDAQMTVWTGDOKFXEEMVAPKDHKEGXPDIPHTKTLHAYWDQXDXKLHNIXNTQXSXLZSUOMCLHLWHIXBEPIKTEXQFIPILEFESLEHNIXPIMHHEHMHNHMLACLPGLFLDFUTDTAALOMCLHLWHLKETGEPGBDTAALKEHSWKKGNQLCHEQXDGXUHEHNIXBETMQEPIMHAYMXLMELNBXHVGTAALKEHSWKELMETMHMTMQEMAQEHETNKUZASQKAHETSTNANQEETMRHQKPETPKEOHEHMHNIXFDFPQXAZFNKPWKQXDSMVOQMVALIRELTAXHIRCGAVPOSVLHTHEXQRQEAZDFPLELMVGXHLWYQMQGBEFTESLEHMUXELKEEGIXGXHLPHYGLHETZTZLTAAHELXINQHEGPLMLDFUAQBDUPHGRALNPOEMZATACLETMKHMLCKGBDQEHVTHLDEMSYAFAPHETHLXHLMWGFDFEXKNELWELALNABHETNIZEOQXSILBZSLDOTGKRYHNIXVAUAAPKFKPSYQMHETHELXHHOQMVASHGSEHQXLCPGNQDFAQIPLCZLXGMQHEQMGFKPPGSWWKELKSQFHLGEVAELAZWQPUMNEXVAQPFTQMEXGEEPGPLBLAAUHBIXLXHNMAKGEMVXLNKPQNMKYPPAHQMHTAGXQMHETHHEQNEXXHRXLTSYXDTSUGALZVUPHGELGQMEAVANQNTHTAUOSVLHTHNTQXSIEPGPHCFDKDQMLCHEADPKQFOGBEELKGBESHWKAYPXTGAMFUZAQXLCHXQGAMSQALEXKEAMIGGQXEMIQLHGZRGUDTHETHSEMQSLXAMAMVWZVAHSQMDFZTAMKPWKRQMQHSXGPWKPFDHEQXCKPOEOOFMAEVLHGOHIMHUGZGLNKPUKYOFDNBHYKLIXCGEQTHATVATMQEPQSAOAAMAUDHUKYPMAULRAPOEONTDTALWVTHQXCAAYRALSRUETSFRUGEIHEMHELDEOSEWEIODAMNMKYPPAHQHSPOEMHEQNQGOELTEMXHHOQMPLNPMKYPPAHQVAGFGOPKCLQMLCHEAMFPHELEEGNTQELYSADACNIHKGPSALHLVASHXDHMELTAPGHEPOKAHELEEGNTQEGTAFALGEPQSAOAHNETHLMTVHETHBIXELXHVMTHHAQMELLYSWSYQMLCAYVGHSEXGMLHPLWLDPLEPFQXKAHNIXQSISQXQXCAAYXDRXAYKTELETMETMHMLKMLCNLNKPTNTDLIMAELGQMEHTSFSMCPLDXUSESGXEAZDFIXELFOAFALGQBECLELKMZSHNHIPLFQVNHMLPYPHELNYSVAHEQXKAAMHXEXGQECQGBEQSSMCPLEGXPDGOXHVAELHTWBWZGTHEQMVSCLHLCEETEVKPXQXDZAXHMXKFXGABAZXDDFAYXSHSMQFNTAAEHNIXPIMHZAXHVAELXINQDFAQHEEGHEAMESQNHSGYXDXIPKQFGQAVHQAMRAGFGPIGMNMKYPPAHQUPQOHUHETDTHGQMEEVCPAQAZIPACTSLEQSIXHLMWUPGDXHVAAYMXKPSETOTHNTETSZPOMPMKYPPAHQFKEMHMQMHVQZXDLCFOAFAEQSMAULLCDAHEHMELALHEQSMAULQXLCHELEPOMAELXHXAVAUAEOLHHMSQEQMECLLCNQBEUGXEWQHEQXCAKLGXXYNLPMMGYPPAHQETKEEGEXZGQEKPSEEOHIRALHPUKEQSCPHMGQFBEQSHAFATFCZLPMMXANECGFKPVSPKFTQNRXZAAWELMKLIKAHLSHEMLKNKQOALKYEGALHSBEEXHNFKMKRAEXEVMKYPPAHQHVQACEGLVZFDMPTAHUHYQEOQOEHQETCNANQEFOABLCNTKEHNQEAZBECLELAUSZXDPKDPQXAZNQLCGTZVEHELATVAMHFPVHDFHEANTMQEQXDXHNXIEMXUXEAFHUXZMKXHZVELMVTMHMKHELMHETMTMHFPVHQMHETHHEQETHUGXMKFAPETMTNTQENTETSZXDMTWKQFIPILAFHULCGEIHAHLKIOLKFHMXKPSEAFHULYBETHXQKAHTEMHSLEHSOEQHMTMVANQEQXGEUHGSEHHEHMLETSTNANQELYEMMHGMPLXGKAAZXDPGBLELMAXZMKPXHUQXSGEQMTWKGQMHVZUGXMQXDTPIWMGXANANMLVHXIMHQFTXALLCANFUIGFNYKHELDFHRATSAMQOMQFEZKETXDQMHEAQMVALLMQXOSTHHLMWHEQEHNVMLTMQSHAFUPNHKEQSMAULISSYENGPEVIRHLSYPOXIEMFDFKMTVHGUQSVDOIXBXUFNZAEHELNHTHELSKGUXDLCNTEXQRKPAMLKNHMVPLKFAPLCXQKAAZQSNHAFAHQMXIQGHEHNLTHEHMSEXQOGBEDWKFTXPOABHETHFZAZAVFDLCFEZHELKFAPHETHETMTNTQETGAZXDGOOEZHGOHISZHNHMXIPXHSLSHSHTRGQEHZKPGRAYMHEXGNOQEMANLETSTNANQERLDFQXSGBECLLAEPLHETAZXMHLEGPLHEHMIGXQSMDPGXQMQHVAHMGEZHELZRLEEGEGKFFMPOPKXPLKCLQXSXHTMVMLWYLSVSLDFULETSTNANQEDTALWVTHQXCXDFXUMHXQKAHLHSHUZAMXCLQFAZEFANHBANHDLPHOVXZLZGEXSMDPGXLTNHEBGSEHLCXQKAEVMKYPPAHQXILBPKQTXQWEGXHSVDETYSRAGFCLQXSXHTMVTAUPMTVWSYHTQXKFAPLUQZXDWZGEUHGSEHRQVAHMUGIPMLPFALQXOTGLGRTAUPMTVHELFUTGLTEMHXAYVSHMHXAYVSHMTXPOABHELMCLHLMVPMMGYPPAHQGTNQQXLCHELAZSQXKSGFDPGTSWWKQXCAFKOZSVPLHLIGHBIXFDCGGOELKETSLHGPHIPGNQHEQXCAKLHMELOTLTMHKEGXHEPKTHEQMRPOPAQHMSLHQFGIMQHSUKYLTSQEHELTMKWPDPUKYPXGVAHMATHLHUETMTUKILRALEEGANMLVZQMPMMGYPPAHQUPGDQMRAGKDHGEEMEXKSIHBLHMTAAHELQWKPSEAFHUSMLHQEMQGMELGQMEHETSLTXGVAHMFDRAAMIGGMETMSHUHYUWQFWQVAOLLPBEELEQXRPMOQMVALQRQPFTQMKFAPRAGFCLQXSXHTMVEXCEELMHNHMHTACLPLLOFBWQUPGDQXOSLDFUAQBEKFBEGOHIPGMXLSMLMNMVOQMVALKHLAAUZIVAHEPOKAEVHINTZAXHXAPGNQHEQXCAGOKFZAYKPODWKFELPHCLPMMGYPPAHQXGSFMLKEHMHLTHYWPOKAFOMVQMAUSVPMOQMVALKHDFMQMHKNELHEHMELGEMHCELAAEHMELKELTMKHEQEESLMCLHLWYQMTDQGQMELGQMEECHSAQXMHLEGELXIQGIXGTPITAHUIXELKGOUCEELYSPGWEQMNTTXPOECQOALIRISQEKFFKOUMEHEAQPISFFPMAPGXIQGPMMGYPPAHQVAUXLUKHETAVAYMXESLTSIQXLKXHMKGXBEZAETSWWKXEVAZKDPPDFBXENQUXUKILRGNQKLQHXAXIQGPMOQMVALKYGXELHSAVQXGYXDLKSWSYFTIWQHXGUIZALTKSANLEQMQGBEXIIHFDHEHMFKMKDFHEAMZFQAVZIXHEHQNHBEOFVAIGMVLCNTKNAYALPMMGYPPAHQXHXGBEELXTHEPKDPPMOQMVALZKMHVLLCHETNQMPKDPXYEMKFEXOMANHMQMOGNFQXLCHELNPKBESIMKQEHETDTHXHXAVAUAAHELMHZAXHXAVAHSQXCOKFFMSYMTECSYMTIXHEPOKAZAXHRXIGAZXDLPMVDPLHAYXDXHRAAQSESGXQXDHEQXSXKGOUGEAFAHAYRATSLTWQHEQXCAGOKFZAEHELFPABHLMVUXZAGQGQXUACCLPOABHETHHEHQNHMHMHATHLCEGLSLYSPLNHAFAEQMQGBEHEQXRYTDPOEONTHSZAHEQMYPPAHQXSCLQXLCNTMNMVOQMVALUWLAATPAANLMUIZGOHZWZLPMOQMVALUHHIHXHGLHYPXQXDZATAUPMTSYWEGXSQEMAYPAIXZVDPLPVHQXCALKIOEHNTLPMHELNLAFATPAANLMXHVAETHLMTXQBLELFPABHLMVNHMHQXPCTPQMHEHMHNIXFDMHIXDFLPVHELVEGKDPQELTWYQSEXMNMVOQMVALZHELFPABHLMVDWHNMTWKNHAFHFETHELTEMMLLZXQTHLKIOEHTXPOABHEQNEXCEELYSGYEMELKGOUMEAVANLEKFELEXOMLHQFGIKGOUOCLHSQNAOQSUXEWQHEQXCAETEVGSEHNTCGQXCGWEHQHXEQGEEMLZMWQMCPHMZAKGOUMEHTXBNLVZHEQNLKBRHMKHPKXDELXHVPMKYPPAHQSQKAHETSTNANQEKMUXAZXDQXLCEXQFLTRIPAANLMFZABHETDTHDFHEHNTAUPZLXGMQXHXARAKFQXDXGPGSFDXPALLMQXAMXGHBIXXGABAZXDIXVAUAATXIVATHQLZAMAQHPXGAQMQFFTQXGYXDHUDFHELNHSKGMWHMPLSMZSLHKMZSAQECQGBEPGPQKTIXUIZSHMHYQETGHSOGKPPAESNQGQBEELEQBAVAMHLHFDWHELBEFKKFAPRXGFPFQMCPHMELEGQXXLVZZAXHMXLTPHQRQGXQKAZTLNKPLHELGTEVCPQMTHTAATSEXESFMLHSQMDFHETDKPEQVHELGTHEEGNTQEXHZVAYXDLSMLHSQMPGPIGNMQFEIHEMXGALBEHUUKQOETMTHEPOKAHEQMZIVAFPSFMLOGZLPLHEADPKQFCEELGTAVHTUAHBZAKTQMEXGQAVHQAMXESWPKNHMECLAYXDAUDHHEGXSEWEEGTMHMNTQEMAQEQXSMZSLHKMZSLEHNIXHTAFAHAYXEEMMTWKPUGQQOSGXDWZHEAMUAMTPKWLGXETYSEXCNLTMKHYZGYHHMTNCLEADFDAFDIOEHCLZOGYBEKLGXNTAHELXHRXLTSYXDUPXDPKNTXIFOMSALOTGLRHAYKTRXLMABHEADPKQFGEEMAYKAELLAQMFZKDALCNGFCLRAGXFTQLHQAMNHMHAUKAZTSYKAHTEMVSHSOHQXCXLEQXKETANPGFDFVSTDHTOTAMEXKEGXFDMAXHVRHMUHDFSIEMKVGFGDQMIXHEPOKAZAETCNANQEWVGDQETHALIXABHBZGLHAYVPEXMXESHNIXTAFZMGQPFTQMKPLTTFIPOQVNALOGMHGQMEAVANQNLCMHTAGXLHETHELEEGZIVAHSSYMTGQXEVAMHLHHYHMANTMHMZHAYXDWPDPAYMXESLHKLGXFCCLRXIXQFNHTODPLEHNIXFZRIPYSNSESGXDQXAYVGUPHGUPGDQXOXKPPGNQHEQXCXZLELGQGMANQNLCMHTAGXLEHNIXNTQXKXTHKTQMNTGTIPLELAGFGDQMOFPIGNMQFEIHABHETDTHHYZGYHIXVAUAAPHTSYXDTHAYPNPKVEELCLELMHEMPLHEAMHVANLHLPMVDPHMLTPGBEELXGKALCBLELGTAVANQNQMLCESIPLEQSELKTZOOHQMEXMNZLHLMHGQRAPOEOETMTDWKFWELEEGLPQFKNETHEHNIXUPGDQXOXKPQXAYXGXMQGLMGKDHAZAVANQNQMLCNTIXUAMTVKGSHSLHHLAUKAHLWYLNAUKDQMZAPFQEELEOZAOFQXHELTYSEXOKAUKDQMZAHEQELTMHVAVAMHLHATPSNHBEPOHBZAETAUABHALMPFELOTZGDHGQHTSIQXHEQEANHAESFLAUKDHMQMQXLCGEWREQXAVANHTPLHQSAMELOTZGDHCEELFOLCZLHMQFAZAHELDFHUAUKAAVALBLQXHEHNLKALVAMHLHNHMHHBCLQXURQXSMZGGRQXHEQMGXHTBDHNAYKTNHMHHEANHQAMPLHETDTHXHZVAYXDAYSQXLWQDFLAGFGDQMPOLCBLELYSXYEMKFFDNHMTFWLTKQHQQMPMMGYPPAHQHEHQFKOUMEZTLTFTLHGPANLTWQHEQXCAETHBIXETSFMLXQXDOGNFDFHELMTSQNQEECQPFTQMKPAMAUSFMLCEELFOLCZLHMXTKDQXXGMQAYVGUPHGEXGMLHPLNOKFBEELVAMHLHLCXHMKMXQPNTPWPOWHELMHELXIECKFFDBEELXHAFEFANABLCHETDTHELGQMEHAGFGDTHZAFZHTBLHMESDPQEHEAMFPDHLCZAXLBDIRANAQXDUKYLHMLMPKNLXAPGMPKCDFISTAAELHYPEQCEGPSQALTHHELHTXWZFZAZHEEGCGEQQXVALTKEHNIXVPUAQXSIHTSHHEHMMAMTMHUPGDQXKXDPEXHYKFIXNHHSQXSXUIHSADATXAMAMAAIVZHUHEAMETMLPLHEQNHSGYXDVAELGTHEEGETGEPKQFGQAVHQAMRALHGFKFIXNHHSQXSIOTGLGHEQNQSHEODFLEHMFTTGRYIGWHIXKMHXXQBEGLAZKAZTQFRALAGFGDQMGQVAQXVZHUPYXBLUQMLKNKQGUKYOFDXYHBIXNQRALTRGQMRQMQHSSMPLAMPGSYMTEQMTMVANQETGTHXGAVGPAZXBLUIWUKQONTVAUXXUWUPOCNANQEXGABAZXDDFTXSYKDXHAFATAFEOHIXIQGSMPLAMPGMPKCDFISTAATAFEOHIHYQEUKZOPOEOETMTNTQEDTALWVTHQXSGPQVAETMTSLXAMAGEOGQTFXLTVAXIEMSLVHQAPGENKHHIELMHSMPLAMPGMPKCDFISTAAPXQXBNLGEXDSYHUKLQHMAMTWKDFAMDTALWVTHQXSIAFHPGSEHRAAMIGGQPSTHQABEHUUKQOHEQXCHELQKNTTXZAPDMHGTMHLOTFZLFDTMQEHEQNIOOAAMETMTFDAZDTGMDPLHAYXDXSGUXDDFZAXHPGBEELYSEQXRRAAQHMDHKEHMELEGXTKDTHHEQMYPPAHQMGHSOHZSQXKSGFDPXYEMKFYALTMKZALUGKGRPLKFAPRAGFCLQXSXHTMVNHAFAHELKWQECLKGPSALHLHUVAOFQGHEHQNHMHFCQFCEDFCLZGAMDPLHAYXDRAGFCLQXSXHTMVOGNFQXDHBEUATFLHHETHXHMGQMTAIPGQSAOALEQETMHMETMNZOARQEMAUKZOEXZTATNQHEQNXIQGOQVNALOGMHDABEHUNHMTETOMMHGZPOPAZAHALHGKLATNSHHLLPMHALMTWQLTMVYGFDBHETAVIGOMPKNLXAPGMPKCDFISTAAUSWSYHTFTZWZLHETHMXKPLTPGBEPUGPLDYPELEGVSLDFULTMHNTQXCOKFWMGSEHGTMHALXAPGZLDFHEAMHVANLHXGFWPKEGGEUHGSEHFDHLMTEMMHXAMAGQENIOOATDUPHEAMRXLSSUXDPYPDYPXARALHYWHNIXETMSXGMQXHIROAEXDTTHOQVNALOGMHELMHIXHEPOKALKSUXDELXHXSGUXDLCHLAFAEHMPGNQHEQXCXZLELGQMEAVGPELNHBEDFLXQXLHAYXDZAFKOUCNAQLPBEELMTWKGEIWUKYOFDNBHYGPANQNVAKLTSQMGXLSMLHSQMTHATVAHEQNIOOAAMLPQFOGZLTXPOLZXIAFAUPISFFPMAELMHTAHUETXSDFQMQPFTQMKPAQZVHMHTQXHUMAQNXAPGXIQGOQVNALOGMHNHETMTPQKTLCNTHEEXOWOULPWHPOEOUKZOHSLNKPIXELVWLHALPDXEHYTHIXELVWLHALPDBEELKWLTGYEMPLPQSAOAAMNHLHQSSHHEHMLPEMPLFDHEEXRKPOXIQGSMPLAMPGMPKCDFISTATOPUOEIHVALKIOARELGQMEABHEQXCHAYRXIXHEQNDPQELBKPRAHMNTHAQNDFXIXGXIQHMTXQWUPODWKFHYKLIXCGEQRQMQHSSMPLAMPGMVYPLAIHMAXMZXALMLMVDFAUDHUKYPMAULGTBDTAAEQSWZAYMXESLTAFAHAYRIPODWKFHYDFDFMAXMLNKPLATMQEQHHSXGETMTNTQEHVQZXDLCMLMVILMQMLPFALLCGTAFAEQSWZAYVSPKMLMWESTMPUMQPDVHSMPLAMPGMPKCDFISTAULAUBDELCNZLOQVNALOGMHHYKFIXQFVAZGGYXDHBGPELVWLHALPDXMMAQNQMFDABLCFDAZDTZATAAOLHXAPGKGFXIPQXSGXNHDANLMXIQZXDUKYOFDNBHYGUETMTEQMTMVANQEEXKWLTPGBECFLNSYKAHLEQOGXPHIQXCSPUMQPDVHMXESAQDWKFUKYLTSQEAVIGOMPKNLXAPGMPKCDFISTAAPPOEMQXKATANLAIVSHMTHQMETULEGSQSYXDFZHZPOMHGQXBNLMHBETMHMUKEQDWKFRIPOMHHELDFEUKEQUKYOFDFKETAFHPGSEHPCEOQNKPHBIXWPGSEHQEQMPLUKOLATABHLMPAMIGGNOQVNALOGMHGTEPHUPCEOQNKPHEEGFPNHMVYXUAEFTMHMETMTDFHUNTGTIPHQPOMHLCKFLAEFCFALLCIPLHELSQAVUOKDQZAVGEWRYATSQEZTUORAQMPGPQKTXGBDQNEGESFPPNMHZHPUMNAMELAUDHMNQWHNLTMPOLXPSMPLAMPGMPKCDFISTAAPLKHTRAHSFUGFGDTHOQVNALOGMHEXGMIGCEELKFAPHSQECLAYXDLCHEHMQPPOMVHETHHSLNHUQXSIPKQFKQPODWKFHYTHTMHMUKEQXAXIQZXDTXPOHBYKELMGGXLSMLHSQMTXPOHBETLBQXTAHUVAPFMLKEQSZAMAQNQMHETHSMPLAMPGMPKCDFISTAAEEGMHTGELCEELFPQXAVELXHVPGPHTFBUGIPLCGQVGIPVAELMHTAMHIXDFRALEEGNTQEXHZAQXCGXEKGEOETMKXHAFATAFEOHILPMWAQHEHMIXTGTHFDSHXIFKSEWEEGRALNGAQMOQVNALOGMHXYHEPIKTLSQAVKQXSXHTMHIXRAQMQGFDXYHBIXFUIGBEETHBETHLMTMHMTWKDFHNIXXIQZXDRAHNIXFDACGUXDLCNTAUTMAQLZBEUAOQVNALOGMHLCEOELSYHBIXHVQLOQVNALOGMHLKNHMTWHIXKTGFGPQXSIFDHEHMRAHMNTHAQNDFEXGNGQMECLEXRXHMHYTHHEHQMHXIQZXDRALMMHXAMAOGXQVAETHAIXEBGSEHPCEOQNKPABLZMWQMOFQXCGKMZGRAPUUPHYHNQEABLCXUEMHELMCLHLMVHEHMQPPOSYVAETHAUAIHEMGINQVSCLHLSHMHHSLHETABHEHQMHMQEGOQVNALOGMHFCNHKEGXELEGSMPLAMPGMPKCDFISTAAOIXMLOEUAIHEMGINQXGGTBENTAUTMAQAZGQMEHBEXABLCNTAUTMAQLCETTFIPOQVNALOGMHMHTGELOGZLEXOMTHHLKEHMDFHEAMLKOUMQSYDWKFYGFDHYAMIGKELTSZHUSMPLAMPGMPKCDFISTAAPPCZGLHMHVNALGEXARAHNQELCBEETAVFDHTAFAHELKWAMHIQXKALHSYQMLCGYAFAHELFPABHLMVPGWEHSWKFZHETDPOEOBEELKGOUMEHCUAAHETHAZAHATNKUFDDFHDFDXRHYUKWYKFFZABHEHQMHXIQZXDHETHHYQEELKGOUMEHCUAAEHSWKFPABHLMRPUMQPDVHVSKFHMPGNQLKNWPKDHEXCEETAVHYKYAMCGEQOQVNALOGMHFDGNMQOCUOPEQZAVZAVAPYLNTAHLMHOMPKNLXAPGMPKCDFISTAATBLHMTAAEAMOGEQTAAHELMLPFALELRGUAALKETDPOEOBEGYAFATAUABHATNKUZAXGIPHTVAPOEMQXCGXLAFAHELHEQXSXLCVAPFAYVNZLLKXYBEELXENQPLELTSQEGQKEHSWKPIMRZSHNTDEXDFHUOIAMXAXIQGOQVNALOGMHNHSEQWTMHMDWKFSMPLAMPGMPKCDFISTAUFOUALOGZLTATGLEEXODHMKTQAXLEMGEWBNTGEHEHMHQAMNTEQTHAWELMVMLVZTGALMGQPFTQMKPADTSLTKSLTAVXQXBXLRALHGFGDISPUMQFNTHKTWPDPAYVSGKDHHTEMANESQXQMZAZAXHXIMTWKGOKNTHKTZAETCENHTPLEEXGMFZEBDFQPNTMVQXVALTOEZAHALMATEQAVNHMHPDSZXDHSPOEMHEANQMDAZAPQVAETMTSEMQMAXMLHGOQPFTQMKPLHLKIOTWTDLIMAELFOAZZTTGGYWEGXFPKDLHEXGMIGKEISSYGMATHLGXOFFPMAZAXHRAHNLKLCEOUKIZCNLEHMTNZHELXHIWQHXAXIQGSMPLAMPGMPKCDFISTAATEMQGDFAVOFFPMAUKYPADGUXDLCHLAFEPHNYKUKYPLEHMLDXLAFUFATDTXGMTKGNQLCWVQXKAHSWKLCAYXIQFHTEMQFOTLHELKWLHELDFHUXLSQHUELETPALNEBKFUKQODFEVLTWQPOGTBENQEXHELMLDFUHNLKAUMTELMHKVQAOMPKNLXAPGMPKCDFISTAAUQPSUXDLCELPWANLHEXOMGUBEQXSIEBQPNTPWPOMKQPFTQMKPHQPOGTBEZSTNANQEXHZVAYXDHEQNTAEOHIUKZOPOEOBEXUEMHBPFLDFUHNLKHSLAAMPAYGLQXIEMHEHQMTCGABHEGXPGXQXIHYQSGYKDQXKAGXPDHEHMTAAHELXHQIVLELVAMHLHVGMHESQXOXKPRXANLHRAHSWKFPABHLVKDPLTEMAUMTELMHZAVAELNTVAFUTGLNKPAYPVIGGNOQVNALOGMHXUMPHUAYXIQFHTEMQFOTHNUATFLTFTLHDLFSATQXTMHMZHAYXDLCAYRNELWEAMPUMQSYMTHWZAHLBEELSEALABHLSHALABHLSWMHMLTHQMSMPLAMPGMPKCDFISTAULIGBEHUXGABAZXDXTKDOGNFDFHEHNTAHPLTAFHUOQVNALOGMHUKZLAYWDUKZOEXANFUIGXEAFAHAYXGXEALABHLVHELMAMLPFALXYAFEFTMHMQFMQMVHTEMAYRELATFLNESPOXIALDAEMYXPOEOBENTPIMSSYMAGQBLGOHIXHRGFDNFIXETSWWKFPABHLMKHIQXLOLZMHHEHMHNUATFTNGFGDRXSYABHLXEFCZLETSWWKTMHMZKAYEOQXPOWHKPEOXYAFHOFDHYGXXENQANTGHAIRIGGNOQVNALOGMHUPGDQXCSHMIRHMUGIPHUCPHMHELHPFPLAYRATANPGFDFOAIXMAXGHBPOEONTQEPOKALCLZMWEXZWKURALTONESPOVXLNKPLETDEXXHHOEXCETAOWESPOPXKPPGNQHEQXKAHNDFHLMTWMQNQNNTVKEXHZPOMALEKFPQKTNTABHLPKXBWLLATFADPKXYXDOFHXHIWPDPTAAHETLZBEUAELVMLTKQLCHTDHZASMPLAMPGMPKCDFISTAUPMLEQKEHMPDZLTKETXDQMELMPQXGMXHAFUPNHGEEMHEQEXIQGQHRIAMUKYPHMGSEHPLKGYPMAFZHEKFGXHETNKUDAABAZXDELMHOQVNALOGMHRAANHQQMAYVGUPHGPIGNMQFEIHVALKIOARELHEPOKAHEQNGSEHNTAYGQXDETSWWKQFMQMWLTHEZAETKSQGVXSYXDQXKAQSUKZLAYWDZAXYMALCHVIPHEISSYKNZAARDPLHAYXDIXQSFPVHEXHTVAAYXGFKOUCEPYVAETKSQGXYHERQAUNLXIQGOQVNALOGMHQSFDAVHIQXKAGXELHSAZMXAZBEELSYKALVATDTXIQGSMPLAMPGMPKCDFISTAAOPYOCQXOAZWZLUKZOEXLVMHHLEMELMXCLGTMHALXARAQMDLVAQECEKFETHBIXHETHTAKFPYVNAUXDPGQFKEEGWVGDQEHEAMUAQEDTHSPOEMHEQNZAKSHNVALTGQHUUPQOHMIXHEHQUPGDQMOFEXGNOGNFHEAMHVANLHLPMVDPAMGSFDXLELEGAUKAAZAVNHAFALCEGLPKHSIXHEHQFCHEUPGDQMOFTHHEAMRKEXGELYDAPDLCVWYGLNLAUPZLPLHELTYSEXOEEXMQOGBEELPKEGQXWPDFLCBLELSQBLELPDLCVWYGHNIXLYDAZAXHMXCLAYXDLCHEQNEXXGABAZXDIXHVQGAQHEHNIXTAPDVAHBZGLTVATAATXIFDMPTASEXEEMTHALIXLBZSLHQSAMIXXYMQELUPGDQMXGPSHULCCFGSLCNTTAUPNHGEEMPGXYEOUPXDHTXDALPGXWIPYKFTTGRYIGSHEMNTHSKEQGPDVAPLAYPXTGLELEEGETEMVAELXGQTPLOQVAXZFEQGXIEMAYPXANLHQXHEAQPHLTHEHMFCCLRXHMLAYGTNTXQKPURLQXXGWEGXSTVAPQVGOUHSHSPVELXHRAPUGQXDTXQFOELDXWATWDLHRAISSYGMIGGNOQVNALOGMHPGQFGQXDMHAUTMQMTHATVAEXKNELMHGQKQPODAABHETHPDLCVWYGTNKPPKNHGQLVPKNLXAPGMKQPFTQMKPAMYSXIQGHEADGIBEOTQSXZXDGTMHLOAFHUPLBLELPDLCVWYGLTRAAMFPDHUKQFSXYSZIVXATKDALBEZANQZSADCLAYPVYSFDSMCFALPVNHMHHEHMQEGPYSLKIPHNIXTAPDVAMQVAPKQHCNZLGSCLAYPDZLTAHPGSEHNTLPMHHEQNIOOAAMVAHSHLGMXHMPQXHSPOEMELNLAFATPAANLMIXNHXHPXHUQXCPHMWVGXLCEOQPFTQMKPLTEMSMPLAMPGMPKCDFISTATFQELBKPXHMKCPHMHETNQFOELDXWATWDLHXGXMQGAQIPZBGXZXALXHXIXTWZFCUWIXHTPAANLMQFMQSHLZBLPLQAZTATKDETYSCPHMAYPXKPLELTCEELZKPOEOMALTOZSYPOPAIRETMLOKZLAUDHTXPULCLUGSEHXQXDGXHETHHYHMHNAYVSHMQMSMPLAMPGMPKCDFISTAHUAMXIQGOQVNALOGMHELAFAETSLHETAVGTPWKPTMHMKGOUMEHZPOOGPGNQHEQXSIFCZLZAOQVNALOGMHTMQEUXZGPOEOYXPOEOBEVGHSVGEXKGNQQXIPLNOUYATSLDEQRQMAULTXCPQNUHLNHCEQHNAYKTGXLSHMNLVZSEFPBLELUPEMDFQFMQSKPKQFKNLAAOZSLEQSELMHETKSQGNHCNLHHLSKLHHEGXCPHMXYHEOQVNALOGMHLCGDETSWWKQXAYXIMPXIEMLZMWQMLCXHMKVAELOQMVALIRLKIPTDPOEOZGPOEOGXHICGGOWZLHKLQSXGSHRGQMETKSQGELNTBEAYXSMHTHRAISKIELEGCPHMETSWWKEXOCTSLEQSHYTHPQVAETMTNTQETSHMIRKVTHKTKHAYRGHMKRGXVAELXMQOMQFEKYISSYOELHPOHTLKFHAUDHHXPOEMQMOGSXAWAWAWAYXAMAOMPKNLXAPGMPKCDFISTAHUPOAFHFHGLHELPQSAOAAMXAXAPGSWWKPGWBNTKEISSYCEHGQXCGZLTAHSDAVSCLHLKEEXODHMKTQAXLEMFZWKQXKAGXXLDTQXZAFZAZGBGBGTBEVAEXGQHAUAIHXQESAMMQEGEXFPKPAUABHALEHSWKPLBLHMAUMTXYHEPQSAOAAMQHRIAMZAXIAFTPHMIREGFZACLHISSYFPWQPOMVLAWLISSYOGWHLATFLNPOEMSMPLAMPGMPKCDFISTAHFAYVSHMQMSLABAZXDETKSQGSGXDHMHUDFHELTMPIXOQVNALOGMHVALMMLOGMTVHELUPXKHSMQFNTAATEMXHHOQMLCHELNPKBEOGKPELATQGETSWWKDABEHUDFHEQMGFKPVALMLCGDTALHHLPKZLPLAYVGUPHGLZKDQMZAQXXGMQETSWWKVXATWDLHXIEMHEQEGTNQXTKDLCHELDHEHMHBPLKPLXOUEPQXZLLHELHEMHLDBLELPVLCGOEXOEGFGDQMTHHELAZAHATNQFOELEISSYGMRAPOEOHMXARAGFGDSMPLAMPGMPKCDFISTATFAUWDQMLOSYPOPAIHEMHELHXYWDAUXDAUKAABHETHIPILAFHURADFLNPKNMQPFTQMKPAMHQAMMAQNQMLCETMTCGEQPOHBLAAPIGGNOQVNALOGMHXUXEAFHUHETHVAETHBTMQECFIPQXAMXAVAHIQXKAHMHNQNHIIXNHAFAOGLEMUGQXHETDLATNSHAZDFRILTARIGKEISSYGQXEMTWKPQXBLUQMPCZGAQCNAMACLHHEGXXZDHHXHIDXGSEHSMPLAMPGMPKCDFISTAUFPKNLXAPGMKQPFTQMKPAMYSXYSUXDAYXAVAMHESQXDAQHPGWEGXGIKDLHPAANTMLEISSYGMFYXDAYPVLALPBECLELPDLCVWYGLTEMGYKDQMHEANQESGEQQXLCAUNLXYHEHSGLSYHVGPAQBECLELIGSHEMPLXUBECLELXQKAAZRATAAPANHQPOPGDFQAFSTDLVPKNLXAPGMPKCDFISTAAPIGGNOQVNALOGMHFDGNGQXDLCELMSPKNLXAPGMPKCDFISTATFALHYHMFDMAQXMHFUQKQPFTQMKPLHYPEQGEEMXHHOQMXTKDOGNFHEAMHVANLHDFHETDKPEQWYAMLCSFMLGEEMLCGDPOABHEAMUAMTMSZLPOHLWYTDAUKDQMZADFDTEXCENHTPTNTAAPPLAUKAAVMLCNTGCHCLELYSVAMHLHATPSXAPGHETHSMZSLHKMZSADUPNHGMQOMQFEUKSHXDLTEMELKGOUMNHGLDZLTHTXWZGTAVAUWDQXSIPKQFCEELKGMWHMTHHELDHEHMQEOGBLELVAMHLHELKGOUGQIPAVANLHELFZEMALPLFTEXDHAVDFHEAMHLFPXFQPNTPWPOSKGFGOUOKDETSWWKELPQMPYPQMELLZMWQMDFAYRAANLAEXKNZAETRXGXLKWLGXOTGLRYHNIXCGEQTXMHTQHMOLLUQMHEQELTHEQMDAPGLFSYMTECSYMTHYZGEAHIXGALBEEXCEQGQIEMHMHEAQWDIRRKHETMHMUHIXLVATDTUKYFPOEOANMLVZIXLCXQRAQXCAAYXDVAKLLSMLWEHSWKFPABHLSWPKAFALOGMTSYXMQGLEGXFTEXDHAVXYHEPOHBHGQXOIFPEQVPTAAEEXOKUPMAOGBEELALABHLVWAMQGLEQSEXKEAMALVLDFFDHCFDXYXDELXHXAVSTDGIEFCLDWKFQXKAHNIXXLPDIPFDHCFDXYXDELFKOUCNHNGDQEQXLXHNLKYPVAQSTNQRMVOQMVALIRVGMHESIXRALDMLEQCEELWPDFECGFKPLCFOLCZLHEQNUACWCLHAAMFDVHETHEHNPOEOVSQECEELEQBANLNBNHHDVXAQXDSMGOMQGEEMSUBDELCNKYGXKGIPQXOQOEHQELKGOUMEHCFDBHETHTABHEGXMTWKPDNQBEMLPFALNQLHQXSGXMTDMHHTAFUPMTVHELKGQFHVKHHMLEPUGQXDOFHEAQSKATXAMAXIEMXIQZXDQXLYRAQMPCZGAMLCETSWWKFPABHLVHELFCKHLKAUMTGN

## Kriptanalisis *Hill Cipher* dengan *known-plaintext attack*



Ayumi Yoshida, yang menyukai Conan, cemburu melihat Conan mengirimkan surat kepada Ai Haibara. Oleh karena itu, ketika Conan memintanya mengantarkan surat kepada Ai Haibara, dia melakukan serangan Man-in-the-Middle (MITM) dengan mencoba membaca surat yang dikirimkan Conan. Akan tetapi, Conan yang sudah mengambil mata kuliah IF4020 Kriptografi menyadari pentingnya *confidentiality*. Oleh karena itu, dia menggunakan enkripsi **Hill Cipher,** 3 karakter setiap kali enkripsi, saat menulis suratnya. Di sisi lain, Ayumi mempelajari bahwa surat-surat dari Conan ke Ai selalu dimulai dengan kata “**Hello Ai Haibara**” dan ditutup dengan “**Conan**”. Bantulah Ayumi untuk membaca isi surat dari Conan sehingga dia dapat istirahat dengan tenang!

OZGAURWSCKAEUPEMOZSSQKIUSZYWKLCYHCZQWUJYESKEKCJASGREFNUWPCAKOPGIYQIWWGAJKJCGZXAZLMEQADAMHHEAQSIFOBQAAACSHMACMBMEYSEFHYKWQARSTBIBZOSOCSIOPGUFDYVTYNHQEKQXEKNRGZTKQWUAGKZAAMKEHUAXFSZIOQSAZLIICOGQKAXEGRYUEIICGAWIEMQWUMPUUGMEGZAGRMSLYTHGLSIERQXECYQKGFIDFEGIEQPMUWCTOESAWWIGWZUZUGQUGZMWFSGUAUYJKJCYIGABGUKOMOWUMRKXRWOWMVVKIUQOYKTNCTCQOYKKXGXYWFSYBJOCKYJSYKWKNKYFZAMSQSLUFQCNZWWWSGMIGLEFTCKIOAQAEVEVRERLQXRUHTQJHUYWUXQGSWCYQUMCGQDSQBQTQEIYGWZGSLKHKCYUCAKOQFQKLOEIUPRMTKUTRAQGYKNUHTCGCQWDCSHMACKNSMQZQPPIKTWRLCPBCNKKTHIICCJNCVQERDOMWGGFOYVWTQISLMDTMAPQOYCYHEYHWUJMNPWEMIFPQBTMIHIICWUJYESKEKCJAGGGWAWQOMKCMYDVOFRCIDUWPMJKCRCSSSYVZKOMUWFYCCSBOIMIOGHSNIYIKWHWWVUKJPGZXWRYMTKUTRYFZAWMKCMOBBYUEWUJKGJOHFUILIKZOQGKHKWRZMKAANA

## (Bonus) Kriptanalisis *Affine Cipher*



Eri Kisaki, ibunda dari Ran Mouri, mengirimkan sebuah gambar kepada Mouri Kogoro. Gambar tersebut mengandung sebuah pesan rahasia yang dapat digunakan untuk membuka sebuah brankas. Untuk mengamankan proses pengiriman gambar, dia menggunakan enkripsi **Affine Cipher 256 karakter**, dimana enkripsi dilakukan **per karakter**. Akan tetapi, sayangnya Eri lupa untuk menyimpan kunci m dan b dan meminta Kogoro untuk menemukan kunci tersebut sendiri. Kogoro yang kebingungan meminta bantuan Conan untuk membantunya memecahkan gambar tersebut. Untungnya, Eri masih menyimpan *source code* dalam bahasa Python yang digunakan untuk melakukan enkripsi gambar. Berikut adalah *source code* nya.

| import math  import random  def affine\_cipher(hex\_values, m, b, n):  cipher\_hex = []  for i in range(len(hex\_values)):  C = hex((m \* int(hex\_values[i], 16) + b) % n)  cipher\_hex.append(C)  return cipher\_hex  def read\_image\_to\_hex(image\_path):  try:  with open(image\_path, "rb") as image:  f = image.read()  b = bytearray(f)  array\_of\_hex = [hex(byte) for byte in b]  return array\_of\_hex  except FileNotFoundError:  print("Error: File not found.")  return None  except ValueError as e:  print("Error:", e)  return None  def array\_of\_hex\_to\_bytearray(array\_of\_hex):  bytearray\_data = bytearray()  for hex\_value in array\_of\_hex:  if hex\_value.startswith('0x'):  hex\_value = hex\_value[2:]  byte\_value = int(hex\_value, 16)  bytearray\_data.append(byte\_value)  return bytearray\_data  def create\_file\_from\_bytes(file\_path, bytes\_data):  try:  with open(file\_path, "wb") as file:  file.write(bytes\_data)  print("File berhasil dibuat:", file\_path)  except Exception as e:  print("Error:", e)  def main():  image\_path = "./flag.jpg"  n = 256  b = random.randint(1, n)  m = random.randint(1, n)  while math.gcd(m, n) != 1:  m = random.randint(1, n)  hex\_values = read\_image\_to\_hex(image\_path)  if hex\_values is not None:  cipher\_hex = affine\_cipher(hex\_values, m, b, n)  bytearray\_cipher = array\_of\_hex\_to\_bytearray(cipher\_hex)  create\_file\_from\_bytes("./chall.jpg", bytearray\_cipher)  if \_\_name\_\_ == "\_\_main\_\_":  main() |
| --- |

Perhatikan bahwa nilai b dan m dibuat secara random. Untuk memecahkan gambar ini, anda perlu mencari terlebih dahulu nilai b dan m. Anda **DILARANG menggunakan pendekatan *exhaustive key search***.

Berikut adalah pranala gambar yang sudah dienkripsi:

<https://drive.google.com/file/d/1Lis3KbHz4NKzqYZ5cUnlNby4Zu3z5Bwa/view?usp=sharing>

Setelah berhasil memulihkan gambar, tuliskan pada laporan pesan rahasia yang terdapat pada gambar tersebut. Lampirkan pula kode yang kalian gunakan untuk mendapatkan kembali nilai m dan b serta kode untuk memulihkan gambar!