과제 4. 고전암호 문제 풀이

1. 고전암호 해독

제시된 암호문을 해독하여 키와 평문을 찾아보시오.

1. 시저 암호
2. 모노알파베틱 암호
3. 비즈네르 암호

2. 현대 암호 활용 사례

다음 알고리즘들의 실제 프로그래밍 실행 사례를 제시하시오. 실제 알고리즘은 이해하지 못해도 좋고 프로그래밍 언어는 무엇을 쓰든지 상관없음.

1. 대칭키 암호 (AES 암호)
2. 해쉬함수 (SHA-256)
3. 공개키 암호 (RSA 암호)

암호 해독 과제물 문제

각각의 암호기법으로 암호화한 다음의 암호문을 해독하고 키와 평문을 찾아보시오.

1. 시저 암호

암호문:
QRB WNYQNF UNOC CQN AXXV FRCQXDC JW JWPAH FXAM, WXCFRCQBCJWMRWP. QN BCXYYNM JC CQN XDCNA MXXA CX KNBCXF CQN PANNCRWPB XO CQN BNJBXW XW CQN LUNAT, FQX LXUM JB QN FJB, FJB FJAVNA CQJW BLAXXPN; OXA QN ANCDAWNM CQNV LXAMRJUUH.

2. 모노알파베틱 암호

암호문:
OQBX! Q XTB'K OULB KT ILE KZLK Q CBTH, TM OE THB CBTHVUXRU, HZLK KZUAU QI GLAKQSPVLAVE XULX LYTPK L XTTABLQV. Q OQRZK ZLWU YUUB QBSVQBUX, OEIUVM, KT AURLAX L STMMQBBLQV LI KZU XULXUIK GQUSU TM QATBOTBRUAE QB KZU KALXU. YPK KZU HQIXTO TM TPA LBSUIKTAI QI QB KZU IQOQVU; LBX OE PBZLVVTHUX ZLBXI IZLVV BTK XQIKPAY QK, TA KZU STPBKAE'I XTBU MTA. ETP HQVV KZUAUMTAU GUAOQK OU KT AUGULK, UOGZLKQSLVVE, KZLK OLAVUE HLI LI XULX LI L XTTA-BLQV. KZU XTTA TM ISATTRU'I STPBKQBR-ZTPIU HLI TGUB KZLK ZU OQRZK CUUG ZQI UEU PGTB ZQI SVUAC, HZT QB L XQIOLV VQKKVU SUVV YUETBX, L ITAK TM KLBC, HLI STGEQBR VUKKUAI. ISATTRU ZLX L WUAE IOLVV MQAU, YPK KZU SVUAC'I MQAU HLI IT WUAE OPSZ IOLVVUA KZLK QK VTTCUX VQCU TBU STLV. YPK ZU STPVXB'K AUGVUBQIZ QK, MTA ISATTRU CUGK KZU STLV-YTD QB ZQI THB ATTO; LBX IT IPAUVE LI KZU SVUAC SLOU QB HQKZ KZU IZTWUV, KZU OLIKUA GAUXQSKUX KZLK QK HTPVX YU BUSUIILAE MTA KZUO KT GLAK. HZUAUMTAU KZU SVUAC GPK TB ZQI HZQKU STOMTAKUA, LBX KAQUX KT HLAO ZQOIUVM LK KZU SLBXVU; QB HZQSZ UMMTAK, BTK YUQBR L OLB TM L IKATBR QOLRQBLKQTB, ZU MLQVUX.

3. Vigenère Cipher

힌트: 키길이는 3

암호문:
tstukapzxavxmczhbwkokrbxzgmowvrsglrlvhahhilcisskhbticnakbavysokpbzswgrgiycyms
kpbzavxpfllfopqxzhhnculthysavfllgbuqtyfbhuxzogkqhurnjhmosfvbmosbyktfhalogjwxuh
mvkxycyhqabfvokavgxnfnmthsrulzedolhzphmlwsxwwgngepzrkcpuomzqkvczlcnacyhuha
vbjkburhdwgavxdoespxjoflwgcwlppelogkgmyivrhalvhbflhbwxityhxygbuhalqeviwzkbavmy
sfbzhbgoppkhhbvblhtmlfphfwzolptbagmlsmokxysvoomaskpbzpbbagyycslbalowbdmosklh
alqhsrulqttsbuhxugxpbmosfhwgzhklsmhhmosvvfglfhmhalqhbfmzcflzticnyskzkxyskldtpfb
uumoszhgipdxzogkvtkzbnvmlrtnfxhhypfxpbtiftgwxyfhbbwdvbjvtwokamhmftnuxkaxuogk
phfgplfxnomosklrphffpbzavxpfahbwzogkkbuybuumosbysrlgulthysmosusoslwgyoiaiklhal
ktaskwznnpxpbzssyawgzcephnksbaghcskmzhdwgngnszxuzrjcgnstsswhbwaikuswacfpgtu
haycipqbjsmosuywzohglglvtmoslocizkalfxocesmlwfbngturulfkpsljftjyelrbuhalzttdalomvt
mosppbwvkltowldtssyhqxzfnkrrhgmosrwolzswwcnshxyskzogkukvqxygmyowlgulqttstzdel
bwprcvyxhuevfbvilwozlogakbavpowvowmdolusqahhpaivglppelhhisepsolhahhlbqakiesdkp
bvpdelgtzptyutpbturlhzxoowhbravbuumvrhavxsckkatfckpbmoslafhuuavzwvtmosfpuaam
fhblpcgocnzszhjxvfwlflacapgyptmfqhvylhbwiimsskzhhrsxwqaywlaatzolhzhyrfhmhygavill
vhsrlocnsrturxcsgavxswmazxaobsckdvhtvxoowmwglrypjxzvbszbuulvbmosiysopcnzahurt
fthypxpbzkfnuyturuschkhapflambuhalgmysxaglawkyswbdmvahyfhdgibrwpbzpbapgzhfkl
hpowelvbzzxhbpptxhbwavxioufgtszblrhbhmvpnfhalpxlt