## [3413ICT Network Security](C:\\Documents and Settings\\s995689\\My Documents\\Teaching\\Courses_2013\\Courses_2003\\6216INT_03\\6216inthome.html)

### **Workshop 2A**

|  |
| --- |
| **Part 1 – Reviewing the lecture notes, answer the following questions**   1. What is the difference between a block cipher and a stream cipher? A block cipher is processed in chunks when going through en/decryption. A stream cipher is encrypted/decrypted on a bit/byte basis. 2. DES ciphers are block ciphers. In each step of a DES encryption, a data block of 64 bits is encrypted by using a 56-bit key. Explain how the encryption is processed with the data block and key having different lengths. 3. Suppose a system has 10 legitimate users. To implement a symmetric-key cryptosystem such that any pair of users will share a unique secret key. How many different keys are there for the whole system? 4. Consider a network based on packet switching. Explain how encryption techniques are used to protect the packet header and the data content. 5. Explain why the following are **not** random bit sequences:    * 000000000000000……    * 110110110110110……    * 001010010100101……   **Part 2 – Challenge Exercises**  Try to break the following ciphertext and answer the questions. (Hint: The ciphertext was obtained by encrypting a message using a Caesar cipher)  IXEVZUMXGVNOI ZKINTURUME OY UTK UL ZNK SUYZ CKRR QTUCT  VXUJAIZY UL ZNK OTLUXSGZOUT YKIAXOZE OTJAYZXE   1. What is the encrypting algorithm? A function that uses a key to transform plaintext into cipher text. 2. What is the key you used to recover the plaintext? 3. What is the plaintext (original message)?   **Part 3 – Hands-on Exercise**   1. Install the software CrypTool (V1.4.30 English version) on your computer and answer the following question: 2. Is CrypTool a hacker tool? 3. List some classical ciphers and modern symmetric ciphers that CrypTool contains. 4. Using the Visualization functionality of CrypTool, study how DES works. In the workshop of next week, we will have some exercises on DES encryption.   (CrypTool visualization: CrypTool \ Indiv. Procedures \ Visualization of Algorithms \ AES \ Rijndael Animation).   1. The following ciphertext has been obtained by encrypting the plaintext using a Vigenère Cipher. Recover the original text. You can use the CrypTool to help you.   (Hints: The Vigenère cipher has used three alphabets for the encryption. The original message text has been divided into blocks of length 3. In each block, the first letter is encrypted using the first alphabet; the second letter was encrypted using the second alphabet; and the third letter was encrypted using the third alphabet. Spaces and numbers were unchanged).  .  Tapngwskf Bnjptlujpt  Kq tapngwskf bnjptlujpt, vkf uhofhs cqe thdksjgqu wvf vkf udng nfa wp gqdtbqv dof gfeuzrw ujh ngvtcjf. Vkf mhz kv sgiftuff wp cv b ukbthe qu tgfsgw lgb. B ubnohutld euzrwpiubrkje vzuwfo lt cotq ufhhsthe vr bu d tgfsgw lgb dtbqvrtavugp. Lgb mgqhvk ju do kpqquucqu hddvrs kq ujh tgfvtlua rg c fsasuqvzuwfo. Viquu mhzu dsg vvuffrwjdof vr “ctxug iptff cwucfl” fhdtbqvlpp.    D dqpnqq tapngwskf dtbqvrtavugp ju wig Gbvd Fpfsasukro Uwbpgbtg (EGV). Ujlt ubtvhn wvfu d 56-ckw lgb bpg prhscwfu lo hrvt gjhifthov ppfht: vkf gofewsqqje fpfhcqrl (GFC), elqjhsvhyv emqfl ekbkqjpj (DDF), pwwqww gghedddm (RGD), dof fjrkftwfzw gghedddm (FGD) ppfht. FHT kv gnhykemg evv wig 56-ejv nfa lt pr mqqhgu tvuppj fprvik (jv zbu gfulhphe kq 1977) uq vvtyjxh ctxug iptff cwucflu. D xqul-cupwqe kv uq dqroz vksgh jvhscwjqqt qi EGV uq d ngvtcjf, mqpyq bu Wsksmg GFU. Wsksmg GFU kbu vfxhsco prwjqqt. Vkf hlsuw prwjqq ju noqzo cv 3EGV-FGH (gqu fpfsasu-gqdtbqv-hoeuzrw) bpg vuht vksgh tgsbtdug nfav. Ujh tgfppg prwjqq ju noqzo cv 3EGV-FFH (gqu fpfsasu-fhdtbqv-hoeuzrw) bpg jv kbu vfxhsco wcujcquu wicw bnopy ipt wig xtg rg hupo rog wp vksgh lgbt. Dhdcxtg GFU lt pru erouleguff vvhijelfpw gqu gwom rupvhdvlpp, wig Qbvlppdm Kqtvluwwf qi Tvdofdsfv scq b ernrhukwjqq uq gfxhmqs b phx uwbpgbtg gqu hqyftqngqu euzrwpiubrkz. Vkf Cgwcqdgg Fpfsasukro Uwbpgbtg djrtgq xcv ujh Skmofdfn dmirskwio. Lu comqzt vkf wvft wp ekpqvf c nfa ofpjuj rg glujhs 128, 192, qu 256 ckwt. Vkf nroihs vkf mhz, vkf orsg vfexsg wig hoeuzrwjqq, cww bnvp vkf orsg fposvvdukroco pxhsjhbf lt thrwlsgg gqu fpfsasukro cqe fhdtbqvlpp. DFU lt uopyoz idjploi lo wvf, dxu FHT kv tvlmn xtgg igdwkoz.  Cvzopfvuje Dmirskwiov    Bubnohutld cohqujvknu dsg fpopppoz edmnhe “rxcnld mhz euzrwpubtvhnu.” Lo cvzopfvuje dmirskwiov, ujh tgqegu bpg sgfjrlfpw vuh ekiggufpw dtbqvrhtdqjld mhzu. Hbek vuhs jdt c xoktvg sbku ph nfav, b rxcnld mhz cqe c sskybvh lgb. Ujhtg nfav bth ncwigpbvldcoma ufndugg tq wicw b ohtudhg hoeuzrwff zjvk pph lgb dcq ppoz dh egfsasugg vuloi wig rujhs. Rxcnld mhzu fbp ef hufgoz fltvujdxugg. Ngvtcjfu wp dh tgqu vr ujh pyqft rg vkf rxcnld mhz edo dh fpfsasugg xkwi vkbv nfa dof ronb ujh pyqft lt cemg wp fhdtbqv wigp tkqdg kft sskybvh lgb ju qpv svdojeoz cybkobdof.  C zfno-lprxp svdoje nfa fsasuqvzuwfo lt vkf Tlwgvu, Ukbols, Cgfnpbp (UTC) dmirskwio (gfxhmqsff lo 1970). Kw sgojgv pp wig ibew ujdu kw ju hyvufohma gjhijexmv wp hddvrs xhsa obtjf rujoh owpcgut hrs ihogubvloi nfav. |