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

### **Workshop2A**

|  |
| --- |
| **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?   N = n(n-1)/2 N = 10(10-1)/2 N = 10(9)/2 N = 90/2 N = 45   1. Consider a network based on packet switching. Explain how encryption techniques are used to protect the packet header and the data content.  Data being sent over a network can be encrypted through a point to point or through end to end. In end to end encryption the header is sent in plain text while the message body is encrypted. In point to point all the data is encrypted however the overhead is higher. 2. Explain why the following are **not** random bit sequences:    * 000000000000000……    * 110110110110110……    * 001010010100101……   All of the following sequences have repeating patterns.  **Part 2 – Challenge Exercises**  Try to break the following ciphertextand 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.   CipherText = (PlainTextCharacter + 20) mod 26   1. What is the key you used to recover the plaintext?   Key = 20   1. What is the plaintext (original message)?   CRYPTOGRAPHIC TECHNOLOGY IS ONE OF THE MOST WELL KNOWN  PRODUCTS OF THE INFORMATION SECURITY INDUSTRY  **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?   Is is an e-learning tool which demonstrates various cryptographic techniques such as symmetric encryption, assymetric encryption, etc.   1. List some classical ciphers and modern symmetric ciphers that CrypTool contains.   An example of a classical cipher includes the hill cypher as well as caesar cipher. More modern symmetric ciphers include DES, 3x DES, and AES   1. 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).  .  TapngwskfBnjptlujpt  Kqtapngwskfbnjptlujpt, vkfuhofhscqethdksjgquwvfvkfudngnfawpgqdtbqvdofgfeuzrwujhngvtcjf. Vkfmhzkvsgiftuffwp cv b ukbthequtgfsgwlgb. B ubnohutldeuzrwpiubrkjevzuwfoltcotqufhhsthevrbu d tgfsgwlgbdtbqvrtavugp. Lgbmgqhvkju do kpqquucquhddvrskqujhtgfvtluarg c fsasuqvzuwfo. Viquumhzudsgvvuffrwjdofvr “ctxugiptffcwucfl” fhdtbqvlpp.  D dqpnqqtapngwskfdtbqvrtavugpju wig GbvdFpfsasukroUwbpgbtg (EGV). Ujltubtvhnwvfu d 56-ckw lgbbpgprhscwfu lo hrvtgjhifthovppfht: vkfgofewsqqjefpfhcqrl (GFC), elqjhsvhyvemqflekbkqjpj (DDF), pwwqwwgghedddm (RGD), doffjrkftwfzwgghedddm (FGD) ppfht. FHT kvgnhykemgevv wig 56-ejv nfalt pr mqqhgutvuppjfprvik (jvzbugfulhphekq 1977) uqvvtyjxhctxugiptffcwucflu. D xqul-cupwqekvuqdqrozvksghjvhscwjqqt qi EGV uq d ngvtcjf, mqpyqbuWsksmg GFU. Wsksmg GFU kbuvfxhscoprwjqqt. Vkfhlsuwprwjqqjunoqzo cv 3EGV-FGH (gqufpfsasu-gqdtbqv-hoeuzrw) bpgvuhtvksghtgsbtdugnfav. Ujhtgfppgprwjqqjunoqzo cv 3EGV-FFH (gqufpfsasu-fhdtbqv-hoeuzrw) bpgjvkbuvfxhscowcujcquuwicwbnopyipt wig xtgrghuporogwpvksghlgbt. Dhdcxtg GFU ltpruerouleguffvvhijelfpwgqugwomrupvhdvlpp, wig QbvlppdmKqtvluwwf qi Tvdofdsfvscq b ernrhukwjqquqgfxhmqs b phxuwbpgbtggquhqyftqngqueuzrwpiubrkz. VkfCgwcqdggFpfsasukroUwbpgbtgdjrtgq xcv ujhSkmofdfndmirskwio. Lu comqztvkfwvftwpekpqvf c nfaofpjujrgglujhs 128, 192, qu 256 ckwt. Vkfnroihsvkfmhz, vkforsgvfexsg wig hoeuzrwjqq, cwwbnvpvkforsgfposvvdukrocopxhsjhbfltthrwlsgggqufpfsasukrocqefhdtbqvlpp. DFU ltuopyozidjploi lo wvf, dxu FHT kvtvlmnxtggigdwkoz.  CvzopfvujeDmirskwiov  Bubnohutldcohqujvknudsgfpopppozedmnhe “rxcnldmhzeuzrwpubtvhnu.” Lo cvzopfvujedmirskwiov, ujhtgqegubpgsgfjrlfpwvuhekiggufpwdtbqvrhtdqjldmhzu. Hbekvuhsjdt c xoktvgsbku ph nfav, b rxcnldmhzcqe c sskybvhlgb. Ujhtgnfavbthncwigpbvldcomaufnduggtqwicw b ohtudhghoeuzrwffzjvkpphlgbdcqppoz dh egfsasuggvuloi wig rujhs. Rxcnldmhzufbpefhufgozfltvujdxugg. Ngvtcjfuwp dh tgquvrujhpyqftrgvkfrxcnldmhzedo dh fpfsasuggxkwivkbvnfadofronbujhpyqftltcemgwpfhdtbqvwigptkqdgkftsskybvhlgbjuqpvsvdojeozcybkobdof.  C zfno-lprxpsvdojenfafsasuqvzuwfoltvkfTlwgvu, Ukbols, Cgfnpbp (UTC) dmirskwio (gfxhmqsff lo 1970). Kw sgojgv pp wig ibewujdu kw juhyvufohmagjhijexmvwphddvrsxhsaobtjfrujohowpcgut hrs ihogubvloinfav. |
|  |

SymmetricAlgorithms

Insymmetricalgorithms, thesenderandrecipientusethesamekeytoencryptanddecryptthemessage. Thekeyisreferredto as a sharedorsecretkey. A symmetriccryptographicsystemisalsoreferredtoas a secretkeycryptosystem. Keylengthis an importantfactorinthesecurityof a cryptosystem. Shortkeysaresusceptibleto “bruteforceattack” decryption.

A commonsymmetriccryptosystemis the DataEncryptionStandard (DES). Thissystemuses a 56-bit keyandoperates in fourdifferentmodes: theelectroniccodebook (ECB), ciphertextblockchaining (CBC), outputfeedback (OFB), andciphertextfeedback (CFB) modes. DES isflexiblebut the 56-bit keyis no longerstrongenough (itwasdesignedin 1977) tosurvivebruteforceattacks. A work-aroundistoapplythreeiterations of DES to a message, knownasTriple DES. Triple DES hasseveraloptions. Thefirstoptionisknown as 3DES-EEE (forencrypt-encrypt-encrypt) andusesthreeseparatekeys. Thesecondoptionisknown as 3DES-EDE (forencrypt-decrypt-encrypt) andithasseveralvariantsthatallowfor the useoffromonetothreekeys. Because DES isnotconsideredsufficientforfullprotection, the NationalInstitute of Standardsran a competitiontodevelop a newstandardforgovernmentcryptography. TheAdvancedEncryptionStandardchosen was theRijndaelalgorithm. It allowstheusertochoose a keylengthofeither 128, 192, or 256 bits. Thelongerthekey, themoresecure the encryption, butalsothemorecomputationaloverheadisrequiredforencryptionanddecryption. AES isslowlygaining in use, but DES isstillusedheavily.

AsymmetricAlgorithms

Asymmetricalgorithmsarecommonlycalled “publickeycryptosystems.” In asymmetricalgorithms, thesenderandrecipientusedifferentcryptographickeys. Eachuserhas a uniquepair of keys, a publickeyand a privatekey. Thesekeysaremathematicallyrelatedsothat a messageencryptedwithonekeycanonly be decryptedusing the other. Publickeyscanbefreelydistributed. Messagesto be senttotheownerofthepublickeycan be encryptedwiththatkeyandonlytheownerisabletodecryptthemsinceherprivatekeyisnotpubliclyavailable.

A well-knownpublickeycryptosystemistheRivest, Shamir, Adelman (RSA) algorithm (developed in 1970). It relies on the factthat it isextremelydifficulttofactorverylargeprimenumbers for generatingkeys.