FIT3031
Information and Network Security
Assignment 1 - First Semester 2017

Submission Guidelines

- **Deadline:** Assignment 1 is due on Friday 7th April 2017, 11:55PM.
- **Submission File Format:** Only submitted PDF files are accepted. On various text editor software you can use "Save as PDF" option or use free converters to convert your file to PDF.
  Note: Do not submit a compressed version of the PDF file or a compression of multiple files. Such submissions may risk losing partial or complete assignment marks.
- **Submission Platform:** Caulfield - Electronic submission via Moodle.
- **Required Student Information:** Please include your name and student id within the main PDF file.
- **Filename Format:** Assign-1_FirstName_LastName_SUID.pdf
- **Late Submission Policy:** Submit a special consideration form (available on moodle) to formally request a late submission.
- **Late Submission Penalty:** A late submitted assignment without prior permission will receive a late penalty of a 5% deduction per day (including Saturday and Sunday) or part thereof, after the due date and time.
- **Plagiarism:** It is an academic requirement that your submitted work be original. Zero marks will be awarded for the whole submission if there is any evidence of copying, collaboration, pasting from websites, or copying from textbooks.
  Note: Plagiarism policy applies to all assessments.

Marks

- This assignment is worth **20%** of the total unit marks.
- The assignment is marked out of **100** nominal marks.
- For example if you obtain **60** marks for this assignment, it will contribute $\frac{60}{100} \times 20 = 12$ marks to your final unit grade.

Notes

- You can use the WolframAlpha web site to perform any calculation necessary for this assignment (`http://www.wolframalpha.com/`). A "Pro computation time" is **not** required to answer the questions and if you receive such message from the website it is likely that you are not performing the calculations right or the right calculations.
- In questions related to modular arithmetic do not write the answers in scientific notation, you need to provide all of the digits for any requested parameter (similar to provided values).
- Try small examples (from lecture notes or other resources) to make sure you are using the proper format for the web site and the correct equation before trying the given values.

1. We consider the security services:

   - confidentiality,
   - integrity,
   - authenticity, and
   - non-repudiation

   for a variety of simple protocols using symmetric or asymmetric cryptosystems, in a network environment where the two participants, Alice and Bob, are communicating in the presence of an adversary (attacker with malicious intent) Eve.
   In the following scenarios for each of the four security services, describe whether or not it is achieved, and in either case give reasons.

   (a) $A \rightarrow B : m||h(m)$
   (b) $A \rightarrow B : m||MAC(K_{AB}, m)$
   (c) $A \rightarrow B : E(PU_B, m)$
   (d) $A \rightarrow B : m||E(PR_A, h(m))$
   (e) $A \rightarrow B : E(K_{AB}, m||h(m))$

   Notation: m is the message, $h()$ a cryptographically strong hash function, $E()$ an encryption algorithm corresponding to the specified keys (symmetric for secret key, asymmetric for public/private key), $MAC()$ is a message authentication code algorithm, K_{XY} is a secret key shared between entities X and Y (symmetric algorithm), PU_X is the public key and PR_X the private key of entity X (asymmetric algorithm), $||$ is concatenation function, $X \rightarrow Y$ specifies X sends to Y.

   [20 Marks]

2. Alice and Bob agree to communicate privately via a protocol based on RC4, but they want to avoid using a new secret key for each transmission. Alice and Bob privately agree on a 128-bit key **k**. To encrypt a message **m** consisting of a string of bits, the following procedure is used:

   (a) Choose a 16-bit seed (random value): **r**
   (b) Generate the ciphertext $\mathbf{c} = \mathbf{RC4[h(r)||k]} \oplus \mathbf{m}$ for the message, where $h(r)$ is a cryptographically strong hash function that produces 128-bit message digest of the input
   (c) Send the bit string $\mathbf{h(r)||c}$

   Answer the following:

   (a) Suppose Alice uses this procedure to send a message to Bob. Describe how Bob can recover the message **m**?
   (b) After how many messages should Alice and Bob change the secret key **k** to avoid RC4 key being repeated?
   (c) Does increasing the bit size of the seed **r** make any difference in the previous part of the question? Explain why or why not.

   [20 Marks]

3. Alice is using CFB mode of operation to encrypt a 16KB file to send it to Bob (1KB=1024 bytes).

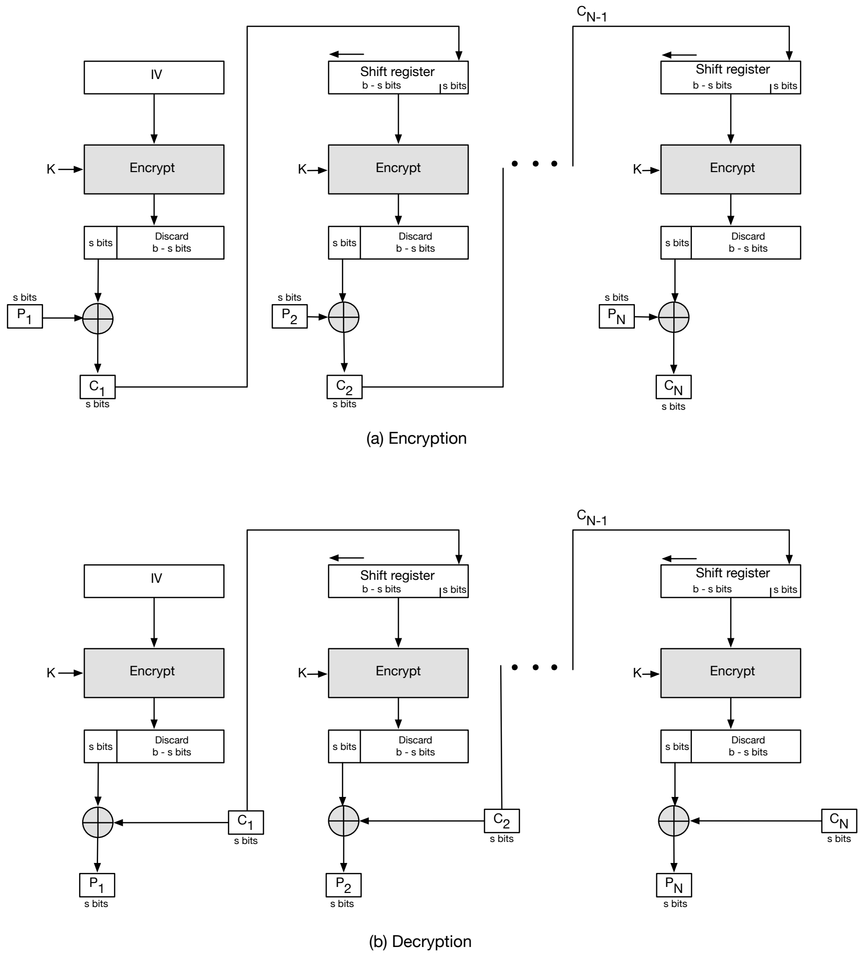

Figure 1: s-bit Cipher Feedback Mode of Operation

(a) How many ciphertext blocks will be produced if Alice uses 8-bit CFB-DES (DES or Data Encryption Standard algorithm as the block cipher in Figure 1)?

(b) How many ciphertext blocks will be produced if Alice uses 16-bit CFB-AES (AES or Advanced Encryption Standard algorithm as the block cipher in Figure 1)?

(c) If there is an error in transmitted ciphertext block C_1, how many plaintext blocks will be corrupted when Bob decrypts the file for 8-bit CFB-DES?

(d) If there is an error in transmitted ciphertext block C_1, how many corrupted plaintext blocks when 16-bit CFB-AES is used?

[20 Marks]

4. Joe is an overworked and under-appreciated programmer at ”This Secure World” company. He is asked to write an RSA key generation algorithm that performs better than the competition. To increase the efficiency of his algorithm he decides instead of generating two random prime factors for the modulus part of every RSA key pair, to reuse one of the previous factors and only generate one new random prime number for the new pair. For instance if the algorithm is generating x RSA key pairs the value of n for these keys would be as:
$n_1 = p_1 \times q_1$
$n_2 = p_2 \times q_1$
$n_3 = p_2 \times q_2$
$n_4 = p_3 \times q_2$
$\ldots$
etc.
This has increased the efficiency of his algorithm by reducing the time required to test the primality of the randomly generated numbers and for the first time in quite a while he is praised by his supervisor for the surprisingly good performing algorithm. The company is going to embed this algorithm in all of their

hardware and software products. You are tasked with evaluation of the security of Joe's approach by either approving or rejecting Joe's idea. For either case you need to provide a compelling argument for or against the explained approach. You can use the following four values of n to argue your case (if needed).

n_1=6707746877476258769687006155346667312135818167434246494098858837590302781071
n_2=10154884310969769321427673109695437709100362015315810046444550032439143118393
n_3=16589923032327209104008156227749326050568372812838589709379351079078499097041
n_4=15754878356255401318163542214784321156924764429187391076177738413008543933383

[20 Marks]

5. Eve (the adversary to Alice and Bob) intercepts the following communication between Alice and Bob:

    - Alice: Let's use Diffie-Hellman key exchange algorithm to share a secret key
    - Bob: Ok, let the prime be $p = 2176403662149810578756025637648768713135196298013160604207149620065458782 2341$ and the primitive root (generator) $g = 5$
    - Alice: Using your selected parameters my public key is $Y_A = 7268937201146768929726789293736151850236699943837892054706367857897711254113$
    - Bob: My public key is $Y_B = 2762341862821258108397201841729140907082340284844672829002911701470020763 21$
    - The rest of the communication is encrypted with K_{AB}

    (a) In the above scenario can Eve recover the shared secret key K_{AB} using the captured messages? Explain what stops Eve from recovering the key or how she can calculate the value of the shared secret.

    (b) Knowing the private key of Alice as $X_A = 278623657769$ what is the value of K_{AB}?

    [20 Marks]