Uva Wellassa University of Sri Lanka
Faculty of Science and Technology
Department of Computer Science and Technology
300 level 1st Semester Examination – May/July 2017
CST332-2 Cryptogrphic Systems

Uva Wellassa University

Instructions to candidates
Duration: Two (02) hours
Number of questions: Four (04)
Mark allocation: 100
Answer all the questions

1.

a. Distinguish active and passive attack with examples. (6 mark)
b. Define "cryptanalysis". (4 mark)
c. Write short notes on followings,
   i. Steganography (4 mark)
   ii. Security services (4 mark)
   iii. Brute-force attack (4 mark)

2.

a. List the advantages and disadvantages of one time pad encryption algorithm. (6 mark)
b. Use "poly vigenere cipher" to encrypt the message "MEET ME TOMORROW", using "university" as the key. (5 mark)
c. Briefly explain the Message Authentication Code (MAC). (6 mark)
d. Compare and contrast symmetric and asymmetric ciphers with appropriate examples. (10 mark)

3.

a. Describe the working process of "F-Function" in DES algorithm. (15 mark)
b.
   i. Define confusion and diffusion. (6 mark)
   ii. Discuss how confusion and diffusion concepts are used in AES algorithm. (6 mark)

4.

a. User A and User B use the Diffie-Hellman key exchange technique, with a common prime P=11 and generator G=7.
   i. If user A has private key a=3, find A's public key? (4 mark)
   ii. If user B has private key b= 6, find B's public key? (4 mark)
   iii. Find the shared secret key? (4 mark)

b. Using RSA algorithm with p=3, q=11, and e=7,
   i. Encrypt the message m=5 (4 mark)
   ii. Decrypt the message which was encrypted in part i (4 mark)
   iii. Find the digital signature for the same message and verify it. (4 mark)

54
115

Table of Laplace Transforms

	$f(t)=\mathcal{L}^{-1}\{F(s)\}$	$F(s)=\mathcal{L}\{f(t)\}$		$f(t)=\mathcal{L}^{-1}\{F(s)\}$	$F(s)=\mathcal{L}\{f(t)\}$
1.	1	$\frac{1}{s}$	2.	e^{at}	$\frac{1}{s-a}$
3.	$t^n,\quad n=1,2,3,\ldots$	$\frac{n!}{s^{n+1}}$	4.	$t^p,\ p>-1$	$\frac{\Gamma(p+1)}{s^{p+1}}$
5.	$\sqrt{t}$	$\frac{\sqrt{\pi}}{2s^{\frac{3}{2}}}$	6.	$t^{n-\frac{1}{2}},\quad n=1,2,3,\ldots$	$\frac{1\cdot3\cdot5\cdots(2n-1)\sqrt{\pi}}{2^n s^{n+\frac{1}{2}}}$
7.	$\sin(at)$	$\frac{a}{s^2+a^2}$	8.	$\cos(at)$	$\frac{s}{s^2+a^2}$
9.	$t\sin(at)$	$\frac{2as}{(s^2+a^2)^2}$	10.	$t\cos(at)$	$\frac{s^2-a^2}{(s^2+a^2)^2}$
11.	$\sin(at)-at\cos(at)$	$\frac{2a^3}{(s^2+a^2)^2}$	12.	$\sin(at)+at\cos(at)$	$\frac{2as^2}{(s^2+a^2)^2}$
13.	$\cos(at)-at\sin(at)$	$\frac{s(s^2-a^2)}{(s^2+a^2)^2}$	14.	$\cos(at)+at\sin(at)$	$\frac{s(s^2+3a^2)}{(s^2+a^2)^2}$
15.	$\sin(at+b)$	$\frac{s\sin(b)+a\cos(b)}{s^2+a^2}$	16.	$\cos(at+b)$	$\frac{s\cos(b)-a\sin(b)}{s^2+a^2}$
17.	$\sinh(at)$	$\frac{a}{s^2-a^2}$	18.	$\cosh(at)$	$\frac{s}{s^2-a^2}$
19.	$e^{at}\sin(bt)$	$\frac{b}{(s-a)^2+b^2}$	20.	$e^{at}\cos(bt)$	$\frac{s-a}{(s-a)^2+b^2}$
21.	$e^{at}\sinh(bt)$	$\frac{b}{(s-a)^2-b^2}$	22.	$e^{at}\cosh(bt)$	$\frac{s-a}{(s-a)^2-b^2}$
23.	$t^n e^{at},\quad n=1,2,3,\ldots$	$\frac{n!}{(s-a)^{n+1}}$	24.	$f(ct)$	$\frac{1}{c}F\left(\frac{s}{c}\right)$
25.	$u_c(t)=u(t-c)$ Heaviside Function	$\frac{e^{-cs}}{s}$	26.	$\delta(t-c)$ Dirac Delta Function	e^{-cs}
27.	$u_c(t)f(t-c)$	$e^{-cs}F(s)$	28.	$u_c(t)g(t)$	$e^{-cs}\mathcal{L}\{g(t+c)\}$
29.	$e^{ct}f(t)$	$F(s-c)$	30.	$t^n f(t),\quad n=1,2,3,\ldots$	$(-1)^n F^{(n)}(s)$
31.	$\frac{1}{t}f(t)$	$\int_s^\infty F(u)\,du$	32.	$\int_0^t f(v)\,dv$	$\frac{F(s)}{s}$
33.	$\int_0^t f(t-\tau)g(\tau)\,d\tau$	$F(s)G(s)$	34.	$f(t+T)=f(t)$	$\frac{\int_0^T e^{-st}f(t)\,dt}{1-e^{-sT}}$
35.	$f'(t)$	$sF(s)-f(0)$	36.	$f''(t)$	$s^2F(s)-sf(0)-f'(0)$
37.	$f^{(n)}(t)$	$s^nF(s)-s^{n-1}f(0)-s^{n-2}f'(0)\cdots-sf^{(n-2)}(0)-f^{(n-1)}(0)$			

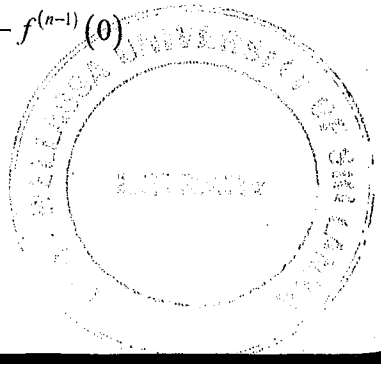

Table Notes

1. This list is not a complete listing of Laplace transforms and only contains some of the more commonly used Laplace transforms and formulas.

2. Recall the definition of hyperbolic functions.

$$\cosh(t) = \frac{\mathbf{e}^{t} + \mathbf{e}^{-t}}{2} \qquad \sinh(t) = \frac{\mathbf{e}^{t} - \mathbf{e}^{-t}}{2}$$

3. Be careful when using "normal" trig function vs. hyperbolic functions. The only difference in the formulas is the "+ a^2" for the "normal" trig functions becomes a "- a^2" for the hyperbolic functions!

4. Formula #4 uses the Gamma function which is defined as

$$\Gamma(t) = \int_0^\infty \mathbf{e}^{-x} x^{t-1}\, dx$$

If n is a positive integer then,

$$\Gamma(n+1) = n!$$

The Gamma function is an extension of the normal factorial function. Here are a couple of quick facts for the Gamma function

$$\Gamma(p+1) = p\Gamma(p)$$

$$p(p+1)(p+2)\cdots(p+n-1) = \frac{\Gamma(p+n)}{\Gamma(p)}$$

$$\Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}$$