CPSC 418 / MATH 318 — Introduction to Cryptography
ASSIGNMENT 3

Name: Harjee Johal
Student ID: 30000668

Problem 1 — Flawed MAC designs, 13 marks

(a) The message M_2 is of the form $M_2 = M_1||X$, where X is an arbitrary n-bit block. From the question description we also know that $M_1 = P_1||P_2||\ldots||P_L$, where $P_1, P_2, \ldots, P_L$ are each n-bit blocks. We can thus think of X as being P_{L+1}. In order to generate a PHMAC message authentication code for this message, we first initialize a hash H with a value of 0^n (n zeros). Then, for each n-bit block in the message, H is updated via $H := f(H, P_i)$, where P_i is the i^{th} block in the message and f is a compression function. Once all the message blocks have been fed into this compression function, the final value of H is output. If we look at the second-last iteration, H is updated via $H := f(H, P_L)$, and in the last iteration, H is updated via $H := f(H, P_{L+1})$, where $P_{L+1} = X$. The value of H after this final iteration is what's output as the value of PHMAC.

If we look at the second-last iteration, the value of H is set to $f(H, P_L)$. Since P_L was the last block of M_1, that means that the value of H generated in this iteration is the value that would have been outputted by the function during the generation of PHMAC(M_1).

(b)

Problem 2 — Fast RSA decryption using Chinese remaindering, 8 marks)

Problem 3 — RSA primes too close together, 18 marks)

(a)

(b)

(c)

(d)

(e)

Problem 4 – The El Gamal public key cryptosystem is not semantically secure, 12 marks

Problem 5 — An IND-CPA, but not IND-CCA secure version of RSA, 12 marks

Problem 6 — An attack on RSA with small decryption exponent, 25 marks

(a)

(b)

(c)

(d)

(e)

(f)

Problem 7 — Universal forgery attack on the El Gamal signature scheme, 12 marks)

(a)

(b)

(c)

Problem 9 — Columnar transposition cryptanalysis, 10 marks