MASENO UNIVERSITY

UNIVERSITY EXAMINATIONS 2016/2017

FOURTH YEAR SECOND SEMESTER EXAMINATIONS FOR THE DEGREE OF BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY

CITY CAMPUS

CIT 404: CRYPTOGRAPHY AND INFORMATION SECURITY

Date: 27th June, 2017 Time: 5.30 - 8.30 pm

INSTRUCTIONS:

- Answer ALL question in SECTION A and any other TWO from SECTION B
- Write your registration number on all sheets of the answer book used.
- Use a NEW PAGE FOR EVERY QUESTION attempted, and indicate number on the space provided on the page of the answer sheet.
- Fasten together all loose answer sheets used.
- No mobile phones in the examination room.

ANSWER QUESTION ONE AND ANY OTHER TWO QUESTIONS.

QUESTION 1 [30 MARKS]

a) List ways in which secret keys can be distributed to two communicating parties. **[6 marks]**

b) What is the difference between a session key and a master key? **[4 marks]**

c) Compare AES to DES. For each of the following elements of DES, indicate the comparable element in AES or explain why it is not needed in AES.

i. XOR of subkey material with the input to the f function **[2 marks]**

ii. XOR of the f function output with the left half of the block **[2 marks]**

iii. The f function **[2 marks]**

iv. Permutation P **[2 marks]**

v. Swapping of halves of the block **[2 marks]**

d) In the Wired Equivalent Privacy protocol used in IEEE 802.11 networks, data are protected at the link level during transmission on a wireless LAN. Each frame has a 32-bit CRC appended to it; it is then encrypted using the RC4 stream cipher, initialised with a shared key and a 24-bit initial value; and finally, the initial value is sent with the encrypted frame.

(i). Describe one passive attack on this system. **[2 marks]**

(ii). Describe one active attack on this system. **[2 marks]**

e) Which parameters and design choices determine the actual algorithm of a Feistel cipher? **[6 marks]**

Question 2 [20 marks]

Block ciphers usually process 64 or 128-bit blocks at a time. To illustrate how their modes of operation work, we can use instead a pseudo-random permutation that operates on the 26 letters of the English alphabet:

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

m	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
EK(m)	P	K	X	C	Y	W	R	S	E	J	U	D	G	O	Z	A	T	N	M	V	F	H	L	I	B	Q

As the XOR operation is not defined on the set {A, . . . , Z}, we replace it here during encryption with modulo-26 addition (e.g., C ⊕ D = F and Y ⊕ C = A).

a) Encrypt the plaintext "TRIPOS" using:

(i) Electronic codebook mode; **[2 marks]**

(ii) Cipher-block chaining (using IV c0 = K); **[4 marks]**

(iii) Output feedback mode (using IV c0 = K). **[4 marks]**

b) Decrypt the ciphertext "BSMILVO" using cipher-block chaining. What operation should replace XOR? **[4 marks]**

c) Your opponent is allowed to send you two plaintext messages M0 and M1, each n letters long. You now pick a new private key K, resulting in a new pseudo-random permutation EK : {A, . . . , Z} ↔ {A, . . . , Z}. You also pick uniformly at random a private bit b ∈ {0, 1} and return a ciphertext C = c0c1 . . . cn, namely the message Mb encrypted with cipher-block chaining using the fresh EK. Finally, your opponent has to guess your bit b. Approximately how large must n be at least for your opponent to have a greater than 75% chance of guessing b correctly? Outline a strategy that your opponent can use to achieve this. **[6 marks]**

Question 3[20 marks]

The RSA public-key crypto system performs calculations in the group Zn, with n = pq being the product of two large prime numbers p and q. The public key consists of the tuple (n, e), with gcd(φ(n), e) = 1, and the corresponding private key is (n, d). A message m ∈ Zn is encrypted via c = me mod n and decrypted as m = cd mod n.

a) Given p, q, and e, how can you apply the extended Euclidian algorithm to find a suitable d? **[6 marks]**

b) If we modified RSA to use as the public modulus a prime number instead of a composite of two large prime numbers, that is n = p instead of n = pq, would this affect its security, and if so how? **[4 marks]**

c) In the UltraSecure virtual-private network, each router knows of each of its remote communication peers the RSA public key (n, e), which all have e = 3 and 21023 ≤ n < 21024. If router Alice needs to establish a shared 256-bit AES secret key k with remote router bob, it looks up bob's (n, e) and then uses this method:

- Alice picks k ∈ {0, 1} 256 by reading 32 bytes from /dev/random
- Alice interprets k as binary integer m with 0 ≤ m < 2 256
- Alice sends c = me mod n to bob
- Bob decrypts c into m and recovers k (by removing leading zeros) Then Alice and Bob secure the rest of their communication with shared secret k.

i. How could an eavesdropper obtain m from c? **[4 marks]**

ii. Suggest a better method of using RSA to establish an AES key than the one given above. **[6 marks]**

Question 4 [20 marks]

Shamir's three-pass protocol enables Alice to send a message m to Bob in the following way:

$A \rightarrow B : m^{ka} \pmod{p}$

$B \rightarrow A : m^{ka\,kb} \pmod{p}$

$A \rightarrow B : m^{kb} \pmod{p}$

a. Explain this protocol, stating the constraint on m and the principal vulnerability. **[10 marks]**

b. It is suggested that the encryption operation $m \rightarrow m^{kx}$ be replaced with a provably secure encryption operation, namely a one-time pad. How would this affect the protocol's security? **[10 marks]**

Question 5 [20 marks]

Describe the purpose of hash functions, message authentication codes and digital signatures, sketching a possible construction for each of them. **[12 marks]**

A funds transfer system authenticates messages between its member banks by having the sending and receiving banks compute a MAC on each message using a key which each pair of correspondent banks in the system establishes monthly using public key techniques. The sending bank then computes a digital signature on the MAC using a long-term signing key. If the MAC is 32 bits long, is this arrangement more, or less, secure than signing a 128-bit hash of the message, and why? **[5 marks]**

To what extent would matters be changed if all messages handled by the system were logged by a trusted third party? **[3 marks]**