IS53012B/A Computer Security

Dr Ida Pu

Room 10, 29 St James
Goldsmiths, University of London

2018-19 (since 2007)

Part I

Homework

Outline

1. Questions

1 Questions

Questions I

1. Consider the Fermat's Little Theorem (necessary condition)

Theorem

If p is a prime number, a is an integer between $(1, p-1)$ (exclude 1 and $p-1$), then

$$a^{p-1} \mod p = 1$$

Fill the missing data in the table below to show it is not true in general if n is not a prime.

n	2	3	4	5	6	7	8	9	10	11	12	13
$n-1$	1	2		4		6	7		9			12
$2^{n-1} \mod n$	0	1										1
$p \in [3, 41]$	3	5		11		17		23		31		41
$2^{n-1} \mod p$	2								19			37

Questions II

2. Give small examples for the following reducibility properties:

$$(a+b) \mod n = [(a \mod n) + (b \mod n)] \mod n$$

$$(a*b) \mod n = [(a \mod n) * (b \mod n)] \mod n$$

3. Perform the following operations using reduction first:
    1. $(273+147) \mod 10$
    2. $(4223+17323) \mod 10$
    3. $(148+14432) \mod 12$
    4. $(2467+461) \mod 12$
    5. $(273*147) \mod 10$
    6. $(4223*17323) \mod 10$
    7. $(148*14432) \mod 12$
    8. $(2467*461) \mod 12$

4. Using shift cipher with a shift of 4 to encode the sentence THE DOG BIT THE MAN.

Questions III

5. Demonstrate how the Vernam cipher works for the example of plaintext "computer" and the one-time pad (5 20 0 9 17 16 22 18). Explain why the cipher is hopeless in practice.
6. Explain how the transposition cipher works. Demonstrate how the plaintext can be decrypted from the ciphertext HKFPRZNIWUVLG UOJOEO TCNMEAOEBOETYCQRXDHDE, using the key IAMTHE.
7. Consider the RSA (Rivest, Shamir and Adleman) cryptosystem. Before sending a message $m = 3$ to Alice, Bob prepares his keys carefully. He randomly chooses $p = 5$, $q = 7$ and $e = 7$. Answer the following questions on the RSA cryptosystem. Show all your work.
   1. What is the value of RSA modulus n?
   2. What is the value of $r = \varphi(n)$?
   3. What is the value of the decryption exponent d?
   4. Which values are used as Bob's *private key*?
   5. Which values are used as Bob's *public key*?