Solution and scheme of Internal Assessment Test 1 – Sept. 2019

Sub:	Cryptography and Network Security					Sub Code:	15TE71	Branch:	TCE
Date:	06/09/2019	Duration:	90 min's	Max Marks:	50	Sem / Sec:	A		OBE

1(a) Solve this using Euclidean Algorithm GCD (1160718174, 316258250).

q	r_1	r_2	r
3	1160718174	316258250	211943424
1	316258250	211943424	104314826
2	211943424	104314826	3313772
31	104314826	3313772	1587894
2	3313772	1587894	137984
11	1587894	137984	70070
1	137984	70070	67917
1	70070	67917	2156
31	67917	2156	1078
2	2156	1078	0
	1078	0	

GCD (1160718174, 316258250) = 1078 **[5 marks]**

1(b) Quote the properties of modular arithmetic.

Properties of modular arithmetic: **[5 marks]**

Property	Expression
Commutative Laws	$(a+b) mod\ n = (b+a)\ mod\ n$ $(a \times b) mod\ n = (b \times a)\ mod\ n$
Associative Laws	$[(a+b)+c] mod\ n = [a+(b+c)] mod\ n$ $[(a \times b) \times c] mod\ n = [a \times (b \times c)] mod\ n$
Distributive Law	$[a \times (b+c)] mod\ n = [(a \times b)+(a \times c)] mod\ n$ $[a+(b \times c)] mod\ n = [(a+b) \times (a+c)] mod\ n$
Identities	$(0+a) mod\ n = a\ mod\ n$ $(1 \times a) mod\ n = a\ mod\ n$
Inverse	$a+b = 0\ mod\ n$ $a \times b = 1\ mod\ n$

2. Find the inverse of the following using extended Euclidean Algorithm
   i. 550 mod 1759
   ii. 17 mod 60

$550^{-1} mod\ 1759 = 355$ **[5 marks]**

q	r_1	r_2	r	t_1	t_2	$t = t_1 - qt_2$
3	1759	550	109	0	1	-3
5	550	109	5	1	-3	16
21	109	5	4	-3	16	-339
1	5	4	1	16	-339	355
4	4	1	0	-339	355	-1759
	1	0		**355**	-1759	

$17^{-1}(mod\ 60) = -7\ mod\ 60 = 53$ **[5 marks]**

q	r_1	r_2	r	t_1	t_2	$t = t_1 - qt_2$
3	60	17	9	0	1	-3
1	17	9	8	1	-3	4
1	9	8	1	-3	4	-7
8	8	1	0	4	-7	60
	1	0		-7	60	

3. Define abelian group and explain its property.

GROUP: **[5 marks for definition of group and abelian group+5 marks for properties]**

1. A group (G) is a set of elements with a binary operation (•) that satisfies four properties (or axioms). It is denoted as **{*G*, • }**
2. A commutative group is also called abelian group . Abelian group is a group in which the operator satisfies the four properties for group plus an extra property i.e. commutativity property.
3. The 4 properties plus commutativity are defined as follows:

(A1) Closure: If a and b belong to G, then $a \cdot b$ is also in G.

(A2) Associative: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all a, b, c in G.

(A3) Identity element: There is an element e in G such that $a \cdot e = e \cdot a = a$ for all a in G.

(A4) Inverse element: For each a in G, there is an element a' in G such that $a \cdot a' = a' \cdot a = e$.

(A5) Commutative: $a.b = b.a$ for all a, b in G

4. Prove that $\langle Z_6, + \rangle$ is a cyclic group and find the generator of this group

Cyclic Group: If a subgroup of a group can be generated using the power of an element, the subgroup is called the cyclic group.

The elements are {0,1,2,34,5}

$0^0 mod\ 6 = 0$

$1^0\ mod\ 6 = 0$
$1^1\ mod\ 6 = 1$
$1^2\ mod\ 6 = (1+1) mod\ 6 = 2$
$1^3\ mod\ 6 = (1+1+1) mod\ 6 = 3$
$1^4\ mod\ 6 = (1+1+1+1) mod\ 6 = 4$
$1^5\ mod\ 6 = (1+1+1+1+1) mod\ 6 = 5$
$1^4\ mod\ 6 = (1+1+1) mod\ 6 = 0\ (repeated)$

$2^0\ mod\ 6 = 0$
$2^1\ mod\ 6 = 2$
$2^2\ mod\ 6 = (2+2) mod\ 6 = 4$
$2^3\ mod\ 6 = (2+2+2) mod\ 6 = 0\ (repeated)$

$3^0\ mod\ 6 = 0$
$3^1\ mod\ 6 = 3$
$3^2\ mod\ 6 = (3+3) mod\ 6 = 0\ (repeated)$

$4^0\ mod\ 6 = 0$
$4^1\ mod\ 6 = 4$
$4^2\ mod\ 6 = (4+4) mod\ 6 = 2$
$4^3\ mod\ 6 = (4+4+4) mod\ 6 = 0\ (repeated)$

$5^0\ mod\ 6 = 0$
$5^1\ mod\ 6 = 5$
$5^2\ mod\ 6 = (5+5) mod\ 6 = 4$
$5^3\ mod\ 6 = (5+5+5) mod\ 6 = 3$
$5^4\ mod\ 6 = (5+5+5+5) mod\ 6 = 2$
$5^3\ mod\ 6 = (5+5+5+5+5) mod\ 6 = 1$
$5^6\ mod\ 6 = (5+5+5+5+5+5) mod\ 6 = 0\ (repeated)$

[8 marks+ generator 2 marks]

Yes $\langle Z_6, + \rangle$ is a cyclic group. The element which can generate the group is called **generator.**
The group $\langle Z_6, + \rangle$ is acyclic group with 2 generators $g = 1\ and\ 5$.

5. Find the inverse of (x^5) in $GF(2^8)$ with irreducible polynomial $(x^8 + x^4 + x^3 + x + 1)$

[GCD -5 marks + inverse 5 marks inverse]

q	r_1	r_2	r	t_1	t_2	t
(x^3)	$(x^8+x^4+x^3+x+1)$	(x^5)	(x^4+x^3+x+1)	(0)	(1)	(x^3)
$(x+1)$	(x^5)	(x^4+x^3+x+1)	(x^3+x^2+1)	(1)	(x^3)	(x^4+x^3+1)
(x)	(x^4+x^3+x+1)	(x^3+x^2+1)	(1)	(x^3)	(x^4+x^3+1)	$(x^5+x^4+x^3+x)$
(x^3+x^2+1)	(x^3+x^2+1)	(1)	(0)	(x^4+x^3+1)	$(x^5+x^4+x^3+x)$	(0)
	(1)	(0)		$(x^5+x^4+x^3+x)$	(0)	

6. (a) Define these following terms
i. Cipher Text
ii. Encryption
iii. Decryption
iv. Cryptanalyst
v. Cryptography

i. **Cipher Text:** The coded message is called cipher text**.** **[1 mark]**
ii. **Encryption:** The process of converting from plain text to cipher text is known as encryption. **[1 mark]**
iii. **Decryption:** The process of turning cipher text back in to plain text is called decryption **[1 mark]**
iv. **Cryptanalyst:** The person who practices cryptanalysis is known as cryptanalyst **[1 mark]**
v. **Cryptography:** The art of keeping message secure is called cryptography. **[1 mark]**

6. b. Find the result of the following
$(a)\ 5^{15}\ mod\ 13$ (b) $456^{17}\ mod\ 17$ (c) $20^{62}\ mod\ 77$ (d) $71^{81}\ mod\ 100$ (e) $60^{160}\ mod\ 187$

a) $5^{15}\ mod\ 13 = (5^{13} mod 13)(5^2 mod 13) = (5 \times 25) mod 13 = 8$ **[1 mark]**
b) $456^{17}\ mod\ 17 = 456\ mod\ 17 = 14$ **[1 mark]**
c) $20^{62}\ mod\ 77 = (20^{60} mod 77)(20^2 mod 77) = 400\ mod\ 77 = 15$ **[1 mark]**
d) $71^{81}\ mod\ 100 = \left(71^{2(40)+1}\ mod\ 100\right) = 71$ **[1 mark]**
e) $60^{160}\ mod\ 187 = 1$ **[1 mark]**

7. Explain the types of cryptanalytic attacks on encrypted messages.

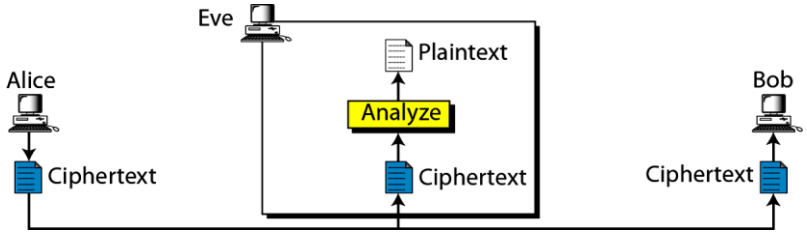
a) Cipher text only attack

b) Known Plain text attack
c) Chosen Plain text attack
d) Adaptive chosen Plain text attack
e) Chosen cipher text attack
f) Rubber-hose cryptanalysis

Cipher text only attack: **[2 mark]**

1. The cryptanalysts has the cipher text of several messages and all these cipher text has been encrypted using same key.
2. The cryptanalyst's job is to recover the key used to decrypt the message with the same key.
   Given: $C_1, C_2, \ldots \ldots C_i$

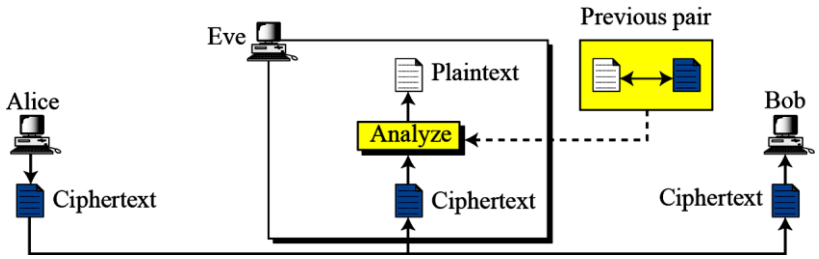
   Deduce: , $P_1, P_2, \ldots . P_i$, $Key \ \ or \ \ an \ Algorithm$



Known Plain text attack: **[2 mark]**

1. The cryptanalysts has access not only to the cipher text of several message, but also the plain text of those messages.
2. Here the cryptanalyst's job is to deduce the key or an algorithm.
   Given: $(P_1, C_1), (P_2, C_2), \ldots . . (P_i, C_i)$

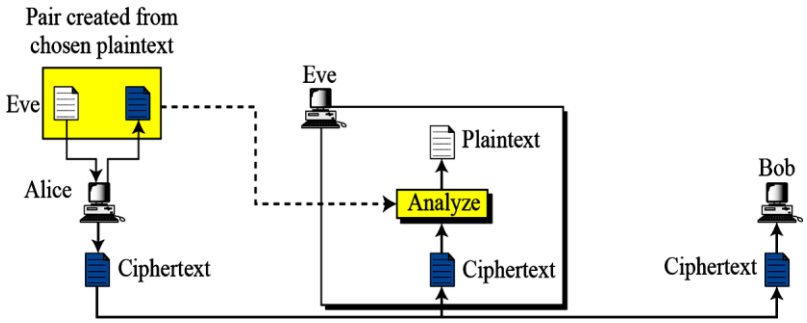
   Deduce: $Key \ \ or \ an \ Algorithm$



Chosen Plain text attack: **[2 mark]**

1. The cryptanalysts not only has access to the cipher text and the associated plaintext, but it also can choose the plain text that gets encrypted.
2. It is more powerful than a known plaintext attack, because the cryptanalysts can choose specific plain text to encrypt, so that one might get more information about the key.
3. Here the cryptanalyst's job is to deduce the key
   Given: $(P_1, C_1), (P_2, C_2), \ldots . . (P_i, C_i)$ where the cryptanalyst gets to choose $P_1, P_2, \ldots . P_i$

   Deduce: $Key \ \ or \ an \ Algorithm$



Adaptive chosen Plain text attack: **[2 mark]**

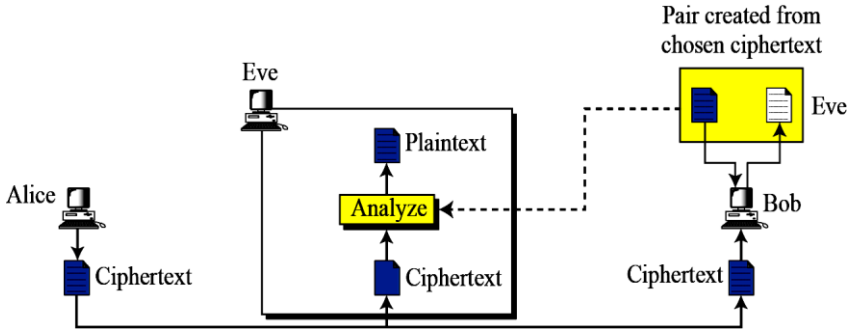
1. This is a special case of a chosen plain text attack, not only can the cryptanalyst chose the plain text that is encrypted, but he also can modify his choice based on the results of the previous encryption.
2. The chosen plain text attack, a cryptanalyst might just be able to choose a large block of plain text to be encrypted, in additive chosen plain text attack, the cryptanalyst can choose a smaller block of plain text and then choose another based on the results of the first.
   Given: $(P_1, C_1), (P_2, C_2), \ldots . (P_i, C_i)$ where the cryptanalyst gets to choose $P_1, P_2, \ldots . P_i$

   Deduce: $Key \ \ or \ an \ Algorithm$

Chosen cipher text attack: **[2 mark]**

1. The cryptanalysts can choose different cipher text to be decrypted and has access to the decrypted plain text.
2. E.g. the cryptanalyst has access to a tamperproof box that does automatic decryption
3. The cryptanalyst job is to deduce the key.
   Given: $C_1, P_1 = D_K(C_1), \ C_2, P_2 = D_K(C_2) \ldots \ldots \ldots C_i, P_i = D_K(C_i)$

   Deduce: Key



Chosen cipher text attack: **[1 mark]**

1. This attack doesn't mean that the cryptanalyst can choose the key; it means he has some knowledge about the relationship between different keys. It is not very practical

Rubber-hose cryptanalysis: **[1 mark]**

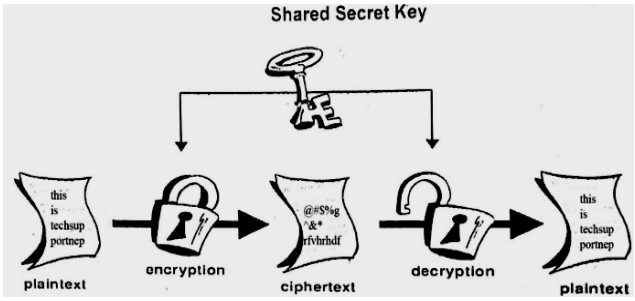
The cryptanalyst threatens blackmails or tortures someone until they give him the key. To bribe someone to get the key is known as purchase key attack. These are very powerful attacks and often the best way to break the algorithm.

8. Define the Term Cryptography. Explain the essential components of conventional encryption.

Explain [6 marks]

1. A cryptographic algorithm is also called as cipher. Generally there are 2 related functions: one for encryption and other for decryption.
2. If the algorithm is based on keeping the algorithm secret, it is known as restricted algorithm.
3. Restricted algorithms had historical interest, but now it is inadequate by today's standard.
4. A large or changing user can't use them, because every time the user leaves the group, everyone else must switch to a different algorithm. Similarly, if accidentally someone reveals the secrets, everyone must change their algorithm.
5. Even more important fact is, restricted algorithm will not allow any quality control or standardization. Every group of users must have their own unique algorithm. Such group can't be purchase commonly available hardware or software products, as an eavesdropper can buy the same product and learn the algorithm. So each group has to write their own algorithms and implementations. If no one in the group is a good cryptographer, then they won't know if they have a secure algorithm.
6. Despite of these drawbacks, it is still a popular for low security applications.
7. Modern cryptography solves this problem with a key denoted by 'K'. The range of possible values of the key is called the key space.
8. Both encryption and decryption use this key 'K', as can be represented as

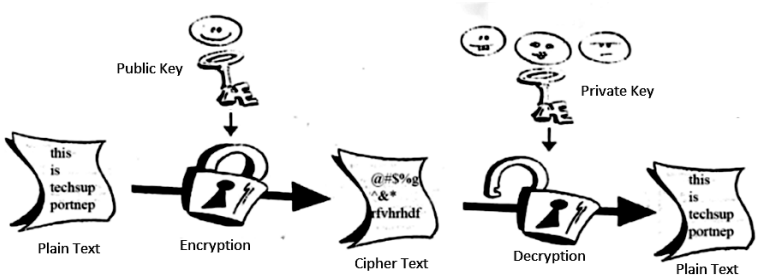
$C = E_K(M) \quad and \;\; M = D_K(C) => M = D_K\big(E_K(M)\big)$



[Figure: Encryption and Decryption using same Key] **[2 marks]**

9. Some algorithm use different key for encryption and decryption.

$$C = E_{K_1}(M) \quad and \;\; M = D_{K_2}(C) => M = D_{K_2}\left(E_{K_1}(M)\right)$$



[Figure: Encryption and Decryption using two different Key] **[2 marks]**

10. The security of these algorithms is based on the key. i.e. algorithm can be published and the eavesdropper may know the algorithm, but if it doesn't know the particular key, it can't read the message.