EXERCISE ANSWER BOOK

(For Personal Use Only)

20180610011012 7 Unit-test-2

Vishwa Chaturvedi

એક્સરસાઇઝ જવાબવહી

(માત્ર અંગત ઉપયોગ માટે)

Subject - Information security

કેન્દ્ર નંબર Centre No.	
પરીક્ષાર્થીની સહી Candidate's Signature	
બેઠક નંબર (આંકડામાં) Seat No. (in Figures)	
બેઠક નંબર (શબ્દોમાં) Seat No. (in Words)	
ખંડ નિરીક્ષકની સહી નામ સાથે Supervisor's Signature with Name	

પરીક્ષાર્થીઓએ સૂચનાઓ વાંચ્યા પછી બારકોડ સ્ટિકર અહીં ચોંટાડવું.
Read the Instructions for candidate and Affix the Barcode Sticker here

વિષય અને કોડ નંબર Subject and Code No.		પરીક્ષાની તારીખ Date of Exam.	જવાબની ભાષા Language of Answer

મુખ્ય જવાબવહી Main Answer Book	પુરવણી Supplement	કુલ Total
1	+	=

પરીક્ષક, સમીક્ષક, કો-ઓર્ડિનેટર અને વેરિફાયર દ્વારા મૂકવાના ગુણ અને સરવાળા મૂકવા માટે આપવામાં આવેલ જુદાંજુદાં ખાનાનો ઉપયોગ કરવો.

Use different columns for marks and total marks given by Examiner, Moderator,Co-ordinator and Verifier.

પ્રશ્નક્રમાંક Question No.	પરીક્ષકે આપેલ ગુણ Marks given by Examiner	પરીક્ષકની સહી Examiner's Signature	પરીક્ષકનો નિમણૂક નં. Appointment No. of Examiner	સમીક્ષકે આપેલ ગુણ Marks given by Moderator	કો-ઑર્ડિ. આપેલ ગુણ Marks given by Co-ordinator	બોર્ડની કચેરીના ઉપયોગ માટે Only for Board office use	
A 1							
B 2							
C 3							
D 4							
E 5							
F 6							
કુલ ગુણ Total Marks — અપૂર્ણાંકમાં In Fractions							
કુલ ગુણ Total Marks — પૂર્ણાંકમાં In Whole Number							
કુલ ગુણ Total Marks — શબ્દોમાં In Words							

મધ્યસ્થ મૂલ્યાંકન કેન્દ્રના વેરિફાયરની સહી Verifier's Sign. of Central Examination Centre		સમીક્ષકની સહી Moderator's Sign.	કો-ઓર્ડિ.ની સહી Co-ordinator's Sign.
વેરિફાયરનો નિમણૂક નંબર Verifier's Appointment No.		સમીક્ષકનો નિમણૂક નં. Moderator's Appointment No.	કો-ઓર્ડિ.નો નિમણૂક નં. Co-ordinator's Appointment No.

સંસ્થાનું નામ / Name of the Institution

બોર્ડની જવાબવહીના માળખાને અનુરૂપ / As per Board's Answer Book

M.R.P. ₹ 6/- (incl. of all taxes) | 16 Pages | smile | Size 20.7 x 27 cm (approx)

Question / Sub-question No.

Q. ___ ___

Q1a – A.

I State a difference between authentication and authorization.

II Which strategy is best for password selection – which is easier to remember and harder to crack?

III What is the key difference b/t strong collision resistance and weak collision resistance?

IV Write the probability formula that among N people at least one person has the same birthday?

Q1 – B.

(I) Briefly define any two standard application of hash function

(II) How HMAC can be used in place of MAC to achieve integrity

Milestone

Question Sub-question No.

Q. III –

(IV) What is an avalanche effect? Calculate CRC for 1100101010110 & div - 100111.

Q2. (A) Salted password verification makes attacker's job more difficult - justify.

(B) Explain the outer round & inner round of tiger hash

Question Sub-question No. ☐ + ☐ + ☐ + ☐ = ☐

Q. ____

Answer.

Q2-B. * Tiger round outer hash :

→ here the input is x.

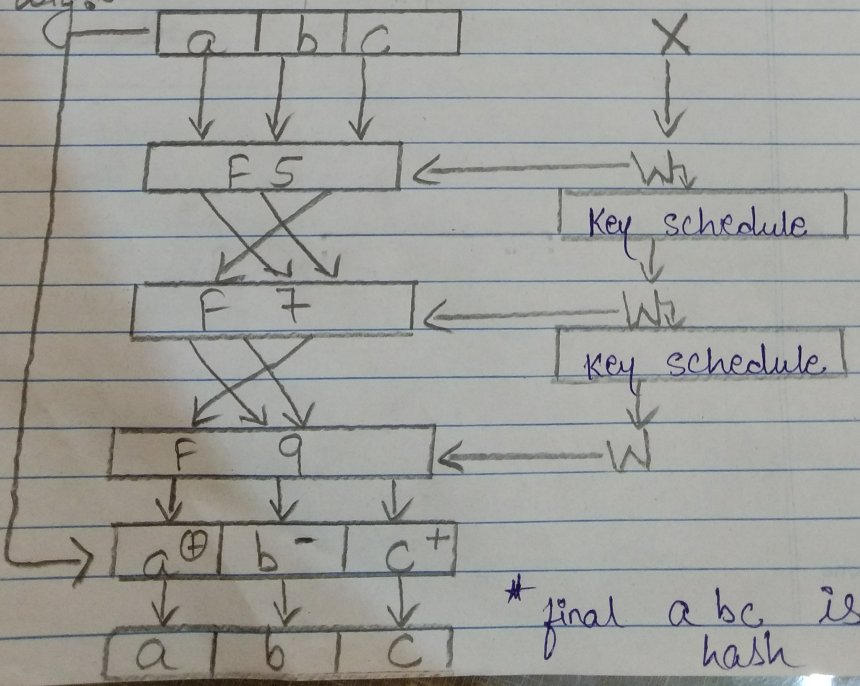
⇒ x = (x_0, x_1 ------ x_{n-1})

→ x is padded.

→ each x_i = 512 bits.

→ it looks like Block cipher.

Dig:-



* final a bc is hash

Milestone

Question
Sub-question No.

Q. ____

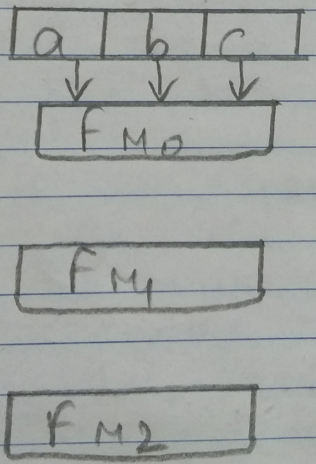
* Tiger inner round.

→ Here each F_M consist of pricesly '8 rounds'.

→ 512 bit- input . W to F_M

Here $W = (W_0, W_1 \ldots\ldots W_7)$
W is the input blocks.

Dig :~



Question Sub-question No.

Q. Q2. (A) Salted password verification makes attackers job more difficult -

Milestone

Question / Sub-question No. [ ] + [ ] + [ ] + [ ] = [ ]

Q. Q1 B I Standard application of hash function.

→ hash functions are used for obtaining integrity.

1. Storing password
2. Digital signature
3. to verify file integrity.

Q1B II HMAC can be used in place of MCA as:-

1. There is No export restrictions for the US.
2. And the cryptographic hash function execute faster in software than other encryption algorithms.

Q1B IV avalanch effect :-

The avalanch effect is the property of the cryptographic algorithm, & typically block ciphers

Milestone

Question / Sub-question No.

Q. ___

and cryptographic hash function.

Q.1a

Ans

T. Difference between authentication and authorization.

Authentication	authorization
① Determine whether access is allowed	① are you allowed to access.
② Authenticate human to machine or either the machine to machine	② Enforces limits on actions.

Milestone

Question / Sub-question No.

Q.

Q1 A. (II) "The password Based on passphrase." this strategy is best for password selection.

Q1 A. (IV) probability formula ⇒

$$1-(365/365)\ \text{----}\ (364/365)$$

$$(365-N+1)/365.$$