2/sept/2024
Monday

lec-9 :-

Hash is collision resistant means secure. Hash fn

(1) if : $m \in \{0,1\}^*$; $H \leftarrow$ given
find : $m' \in \{0,1\}^*$
s.t. $H(m) = H(m')$.
→ if hard prblm. → this property is called "one way image resistance property".
← solvable hai agar !!

(2) given :- $h \in \{0,1\}^\ell$
find :- $m \in \{0,1\}^*$
s.t. $H(m) = h$
→ If hard prblm called Property called "pre image resistance property"

(3) given :- H
find :- (m, m')
s.t. $H(m) = H(m')$
→ If hard prblm called "collision resistance property".

→ what

success. p

prob

assum

such ans do

Random oracle fn

WORK ON preimage calculation ??

Page No. 1

Date: / /

In ① :- want m' whose hash is also same
means m and m' both are preimages of H.

(m) given want (m')
↳ so 2nd preimage.

In ③ :- No constraint,
no msg is given.
~~want only H~~,
Want 2 msg's having hash same.
→ so easiest problem out of 3.
↳ agar isko hi solve nhi kate, baaki kaise hi kroge!

⊙ If Hash fn is collision resistant, then it is both preimage resistant and 2nd preimage resistant.

⊙ attacker problem coincide with ② problem, bcoz u r sending file through channel and digest through whatsapp, then attacker wants to replace that file having digest same as you send it.

⊙ How can prove that 2nd preimage resistant?
↳ Mathematically not possible (especially for symmetric encryption methods ????)
↳ so for them perform statistical test.

Page No.:
Date: / /

For hash f^n → desired property
↳ collision resistant
↳ can be tested statistically.
⇓
If hash f^n follows "random oracle model", then it must be collision resistant.

→ but can't test preimage and 2nd preimage resistant property.
↓
given input/output dataset → but not able to find correlation b/w them (2)

3 properties :-

(1) Any f^n in black box (if not known) is oracle f^n. But Random oracle when follows 3 properties :-
① f^n must be deterministic / repeatability.
(for same Input → same output)

② Independence
↓
can't predict ~~output~~ y_2 from x_2 (single bit of)
↳ while knowing y_1 from x_1.
↳ But can predict
50-50 chance ! Gaa O Ka.
↳ Then how can't predict ?

→ How to evaluate algo wrt accuracy ⇒
by probability of success.
↳ jitni jyada, utni better.
↓
is this correct ??

(1) :-

(2) :-

Work is worship.

Page No.
Date: / /

If ek algo ki prob of success = 0,
duse ki _____ = 0.6

then yeh better!

as 'iski' component always true !!!!

→ so not good measure!

→ calculate deviation :-

$$\Delta(k) = |P(S) - 0.5|$$

(advantage in) ← Δ(k) ← size of input

↳ probability of success.

→ this is only for binary decision making algorithms.

① meaning of independence → even if two inputs are highly correlated?

⇓

(can't predict → single bit of output from 1st output with any significant advantage).

→ advantage of attacker's algo must be negligible.

③ There must be no correlationship b/w input and output, means no correlationship b/w bits of x and bits of y.

WTMK © 3rd.

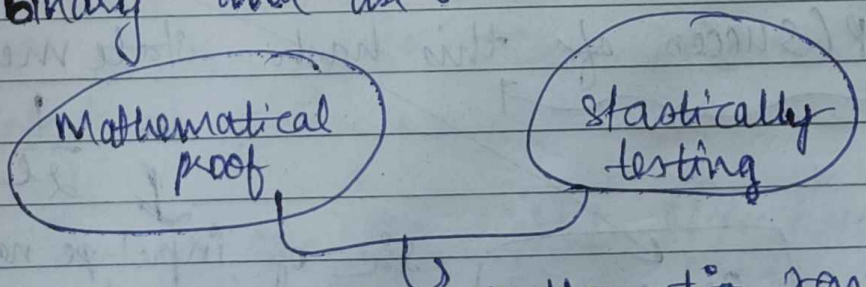
Page No.:
Date: / /

⊛ 7 model to remember / represent these 3 properties.

make table, initially empty.
- take input, toss coin, (like if fail → output = 0, o/w '1', or vice versa) → record in table.
- take another input → scan through table agar hai return value, o/w toss coin, see output, put tuple in table.

① repeatability ✓ → as scanning, so no repeation
② no correlation ✓ → as ② not looking at input, just tossing coin.
③ can't do prediction ✓

→ again binary output na hota, say '6', hota → roll dice → see output → convert into binary and use.



~~mathematical~~ random oracle model. like beech mein bridge ki taah. act karta hai

→ Independence. prop is preserved or not, can be checked through statically testing.

Work

Page No.:
Date:

as $n = 2^l$ (???)

$TC = O\left(\frac{2^l}{2}\right)$

$= O(2^{l-1})$

↓

exponentially.

↓

so can not solve in polynomial time,

$h \leftarrow H(m)$
for (i = 1 to L)
{
$m' \xleftarrow{R} \{0,1\}^n$
if ($H(m') = h$)
return m'
}

→ Now exhaustive se NP problems ban gyi!

$P(S) = \left[1 - \left(1 - \frac{1}{2^l}\right)^C\right]$

↳ nowhere m' is coming.

IFP ki

⊙ To make hash fn which follows random oracle model can be done through statical testing.

Security of RSA digital signature ---> Soundness property (???)

→ 'Integrity' is task of hash fn.

→ ab say 'digest' bhi insecure channel se bhej rhe, but encrypt karke by private key which will be decrypted by receiver's

Work

Page No.:
Date: / /

Thm :- If hash fn follows "Random Oracle model" then follows "collision resistant property".

② $h \leftarrow H(m)$

while (1) {
$m' \xleftarrow{R} \{0,1\}^*$ ← generating randomly
if ($H(m') == h$)
return m'
}

→ Exhaustive search algo.

IFP se different? → (1 to n)
↳ taking sequentially elements from search spaces but here not!
avg no. of iterations = $n/2$ (???)

→ If searching randomly → avg. no. of iterations as best → 1, worst → n ↳ $n/2$

→ If searching sequentially → avg no. of iterations as best → 1, worst → n, ↳ $n/2$

P(success of this hash statement) = $\frac{1}{2^l}$ (and 1 iteration)

↓

size of input pe nahi depend krta ☺

same as each element is equally likely to occur

↳ so chahe randomly kro, chahe sequentially,

say problems (P1) given :- e, n, hash f^n, (m_1, s_1), (m_2, s_2), ... (m_c, s_c)
find :- (m', s') s.t. it is valid pair
i.e. verify $(m', s', e, n) = 1$.
↳ this f^n must always return '1'.

(Computation problem for attacker)

To get my signal, need many other signals, at least 1.
atleast ek-toh ho.
→ jitne jyada pairs, attacker ko utni dis advantage and
channel utna jyada secured.
kitne krein supply?
↳ polynomial number of pairs
'c' pairs,
where $c = poly(k)$.

want to prove that this is "Hard problem",
only then secured hoga RSA DS.
will use "Problem Reduction" to prove soundness of "RSA DS".

Want to show,
RSA encryption problem (P_2) to P1, as
P2 hard as long as IFP problem is hard.

public key.
↳ whatsapp ko thga diya with help of digital signature.
↳ for authenticity and non-repudiability.

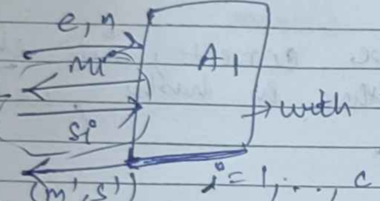
(*) **Soundness analysis of RSA digital signature**

this scheme is ensured as long as
→ RSA encryption scheme is secured (OR as long as) as we use collision resistant f^n in this scheme.
↳ then RSA Digital signature (RSA DS) scheme is secured and sound.
↳ to ensure that, first must know the objective of attacker.
↳ in any digital signature (chahe RSA ho yaa kuch bhi) → objective of attacker is negative/complement of your objective.
i.e.
we are digitally signing the document, we want to secure signature.
↳ attacker objective is to learn the signature, for (digital signature forgery) krega.
↳ in another document, wo sign use krega, which has value to attacker.
↳ able to generate "fetched signature" on some data.

WOMK c 30 mm.

(m, s) → message signature pair

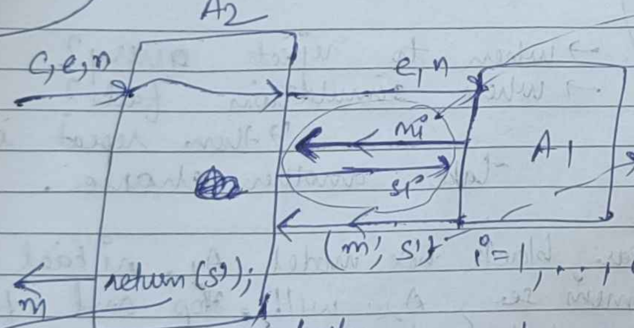
f will call you to give pairs (m', s)
↳ will give 'm' and u will give 's'
↳ this will be done 'c' times.
↳ so will get 'c' pairs.



msg dega correct signature acc do corresponding to it. ↳ 'c' times

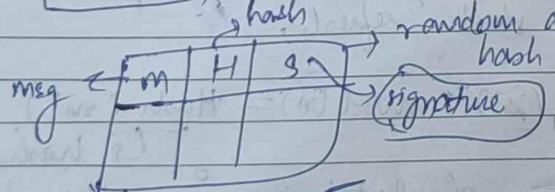
→ with this can design A_2, which can solve P_2.

A_1 → black box.
A_2 can't be, as u have to prove ∃ exist such A_2.



end pe yeh pair nikega

ad s' is itself (m)



→ random oracle hash model / fn.

simulate queries:-

$s_i \xleftarrow{R} \{0,1\}^k$

$h_i \leftarrow (s_i)^e \bmod (n)$

insert $\langle m_i, h_i, s_i \rangle$.

WOMK c 30 mm.

→ if have algo to solve P_1, then by using it as subroutine, can make always a algo to solve P_2.

→ If P_1 is easy then P_2 is easy.
→ can use sol'n of P_1 to solve P_2.
→ If P_1 can be solved in poly time, then P_2 can be solved in poly time.
→ aka CONTRAPOSITIVE:-
If P_2 is hard, then P_1 is hard.
↳ is this hard? → Yes!
↳ this is just our assumption.

→ If can break P_1, then can break IFP problem.
↳ and yeh abhi tak break nhi kr paaye, so P_1 bhi nahi kr skte.

Show:-
P_2 reduces to P_1

Proof:-
assumption:- P_1 can be solved in poly-time with some algo (A_1).

To have:- P_2 can be solved in poly time with some algo A_2.

→ but how I will give s', as uske liye private key chahiye.
→ will generate randomly a s_i, according to length of msg (k).

work $\frac{c}{...}$ m.

value hi wo assign ki hai hash ko ← $h_i \leftarrow (s_i)^e \bmod (n)$

Page No.:
Date: / /

(c) signature is valid ✓, as (hash equal)
random generate ki usse kiya hai.

(d) How generating hash → follows "Random Oracle f^n" ✓

"if s_i is random
then $(s_i)^e$ also random.

everything will be correct, sirf ek triplet get aayega, there in hash, we'll assign 'c'.

M	H	S
m_i	h_i	s_i
	c	

any random triplet

→ How how to return the signature?

→ when to reject query?
→ when simulation fails?
↳ then repeat it, take another chance.

→ agar black box model A_1, nikaal lein beech mein se, A_2 will stop and fail, then start refresh.

$(s')^e \bmod (n) = Hash(m')$
↳ hash value we are simulating in the table.

LOOTMK e
50 ♡♡.

(s') itself is m,

as

$(s')^e \bmod n = \text{Hash}(m') = c.$

$\hookrightarrow ((s')^e)^d \bmod(n) = cd$

$s' = c^d \bmod(n)$

$= m.$

✓.

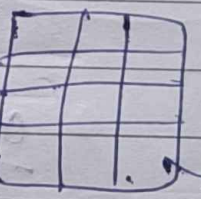
6 Sep 2024
Friday.

Lec-10 :-

non-deterministic algo??? same???

If advantage of algo A_1 is $\epsilon(k)$, then what is advantage of algo A_2 → $\epsilon'(k)$ = ??

→ what is prob that attacker selected the same row



$$\frac{1}{\text{no. of rows in table}}$$

→ row which you have selected.

$$= \frac{1}{(\text{no. of hash queries} + \text{no. of sign "})}$$

→ in worst case, if all distinct, o/w may coincide.

$$= \frac{1}{c_1 + c_2} \quad \text{(say)}$$

so, $\epsilon'(k) = \left(\frac{1}{c_1 + c_2}\right) \epsilon(k)$

$c_1 \in$ poly(k), $c_2 \in$ poly(k)

Page No.:
Date: / /

$c_1 + c_2 \in poly(k)$

so if $\epsilon(k)$ is not negligible, then $\epsilon'(k)$ also not ".

→ if $\epsilon(k)$ negligible, then $\epsilon'(k)$ is also negligible.

Thus RSA prblm is hard,
↳ so our initial assumption that RSA DS is insecure is wrong.

as $\epsilon(k)$ is non-negligible, this $\epsilon'(k)$ also non-negligible.

trap door f'n, 3 gale

→ out of 4 prblms we discussed, which are NP complete and which are not ???
DLP, IFP → NP complete

other two are not NP complete.
↳ RSA, diffie Helmann.

→ as NP prblms can be reduced to NP complete in poly time.

IFP, DLP can not be reduced to any other prblm,
but RSA, Diffie Helmann can be reduced to IFP, DLP thus they are not NP-complete.

Page No.:
Date: / /

(*) security properties of Hash f^n's :-

(1) Preimage
(2) 2nd "
(3) collision resistant
↳ implies both (1) and (2)

(*) If f^n follows random oracle model then it is collision resistant.

MAC algo :-

↳ its soundness property and how it is ensured

Encryption :-

↳ its soundness property and how it is ensured.

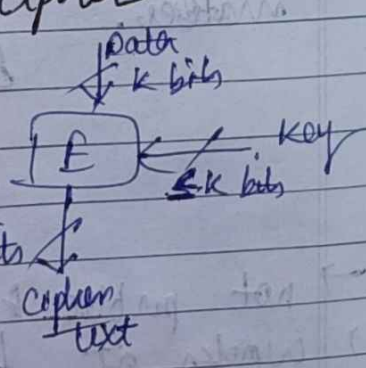
PKI → Public Key Infrastructure

Symmetric Encryption

Block cham cipher

stream cipher

→ Diffusion property ?
→ confusion " ?
↳ bits of key and " " cipher-text mein koi correlation nahi hona chahiye



Work :-

Stream Cipher :-

Key → Random key stream generator → Key stream : 0101011011000...

↳ can take entire file (even of 1 GB) as generatory only key stream

(+) Data stream :- 10110100000 11 ....

Ciphertext stream :- 1100 ....

→ other random fn → just ensures randomness, but does not ensure from sequence of bits ki vaapis seed nikl jaaye

↓

but cryptographic random number generator ensures this

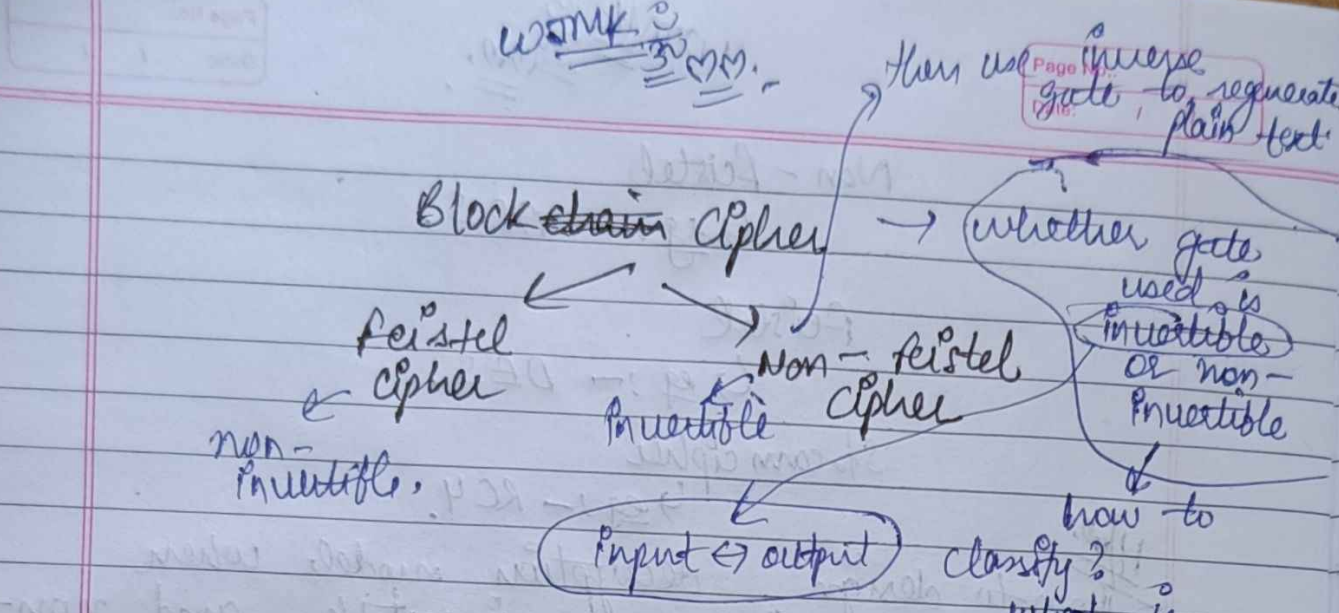
↳ major difference b/w cryptographic random no. generator and other random generator functions.

(**) How to create random f^n generator to generate random numbers in uniform manner.

Block Cipher :-

↳ can take 128 / 256 bits only, not entire file.

→ not public key cryptography
→ works at binary level only
→ ensures diffusion and confusion property.



Gate examples :-

may not be invertible ← COMPRESS → input : 8 bits, output : 4 bits
aka not invertible ← DECOMPRESS → —— 4 —— 8 ——
invertible ✓ ← XOR → 2 input, 1 output
may not be invertible ← LEFT SHIFT → 1 input, 1 output
invertible ✓ ← ROTATE
is it invertible or not ?? ← SUBSTITUTE
↳ permutation / map
↳ map from 4 to 4 bits OR 8 to 8 bits.
Bijective
⇓
Does it mean that it is invertible or not?
↳ NO!
↳ depends on hardness in calculating the inverse!

↓
may or may not be invertible.

→ If block cipher contains only invertible component → then, ↓ Feistel cipher structure.
Non-

→ If block cipher contains mixture of invertible and non-invertible components → then Feistel cipher structure.

Page No.:
Date: / /

Non-Feistel
↳ eg :- AES.

Feistel
↳ eg :- DES.

Stream cipher
↳ eg :- RC4.

Hw.
How to design decryption model when have mixture of invertible and non-invertible components?