POIS

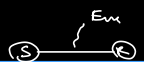
FANTASTIC Q When is a problem Infosec one? [Ans] When the problem is impossible to solve logically / perfectly.

Will be shown with standard examples.

eg1: Hashing password.

theoretically impossible to be perfect if length is not infinite.

eg2: secure communication



@ t_0 info(R) = info(eve)

@ $t > t_0$ info_rec(R) = info_rec(eve)

eg3: Data integrity

If m was sent, modified to m' → It is the same to receiver.

and if m' " " , └ cannot thus identify.

Eg of non infosec → infosec

- problem in distributed computing ∴ now an Infosec problem.

Solution: use signatures. ⇒ implying signatures are impossible.

FASCINATING Q. How to logically solve / circumvent a logical impossibility?

[Ans] Bring in another impossibility and make it destructively interfere with the original one.

We focus on 4-5 sources of impossibilities in the semester.

Course: See impossibilities

Introduce others

Solve them

1 per month approx.

Sources of Impossibility.

① Computational Hardness [Resource Complexity]

② Practical Uncertainties — Only buggy codes are secure.

③ Natural Limits — Speed of light, Quantum Stuff

④ Logical / Philosophical Impossibilities

Random Words

— Hamming Distance

FUNDAMENTAL — •Information security is God — all nontrivial works of science must include info sec

-logical nogo