Date

~ Class Activity ~

Problem: Digital documents can be modified without leaving physical evidence, so traditional time-stamping methods are not sufficient.

Cryptographic Tools: The solution uses collision-resistant hash functions & digital signatures to work with the document's data itself

=> **Two Schemes:-**

1) **Linking Scheme:** Each doc's hash is linked to the previous one, forming a chain of time-stamp certificates. This makes it computationally infeasible for a service to back-date or forge a time-stamp without detection.

2) **Distributed Trust Scheme:** The document hash is used as a seed in a pseudorandom generator to select multiple independent clients who then provide signed time-stamps. This removes the need for a centralized time-stamping authority.

Advantages:

1) make it difficult to forge or alter timestamps
2) supports non-repudiation by providing a reliable record of when doc was originally created
3) reduce storage & bandwidth needs.
4) preserve privacy

These methods can help verify the authenticity of various digital media by ensuring they haven't been tampered with