THE PROBLEM

\[ A, g^x \rightarrow B, g^y \]

\[ g^{xy} \leftarrow g^{xy} \]

Basic Diffie-Hellman Protocol
Once the session keys are destroyed there is no way to recover them, even by the owners,
**BUT NO AUTHENTICATION**

Modified Okamoto-Tanaka Protocol

Identity-based setting:

- Key Generation Center (KGC) chooses safe primes \( p, q \); RSA exponents \( e, d \); generator \( g \) of \( \text{QRN} \) for \( N= pq \). Publishes \( N, g \) and \( e \) (e.g. \( e=3 \)).

- Secret key for party \( I \) is \( S_I = H(I)^d \mod N \) (computed by KGC)

- Ephemeral session values: \( g^x \mod N \) for \( x \) of length twice the security parameter (e.g., between 160-256 bits)

No other 2-message key agreement protocol with a single group element per message is known to achieve PFS against active attacks.

We prove the security of extensions to the protocol that support identity-based authentication between parties that belong to different trust domains without the need for any coordination between the corresponding trusted authorities, a scenario of particular significance in the ITA setting.