UNLOCKING SECURE DATA SHARING WITH PROXY RE-ENCRYPTION

Welcome to our Hackathon project! Discover how Proxy Re-encryption revolutionizes data security and sharing, perfect for large-scale environments like Walmart.

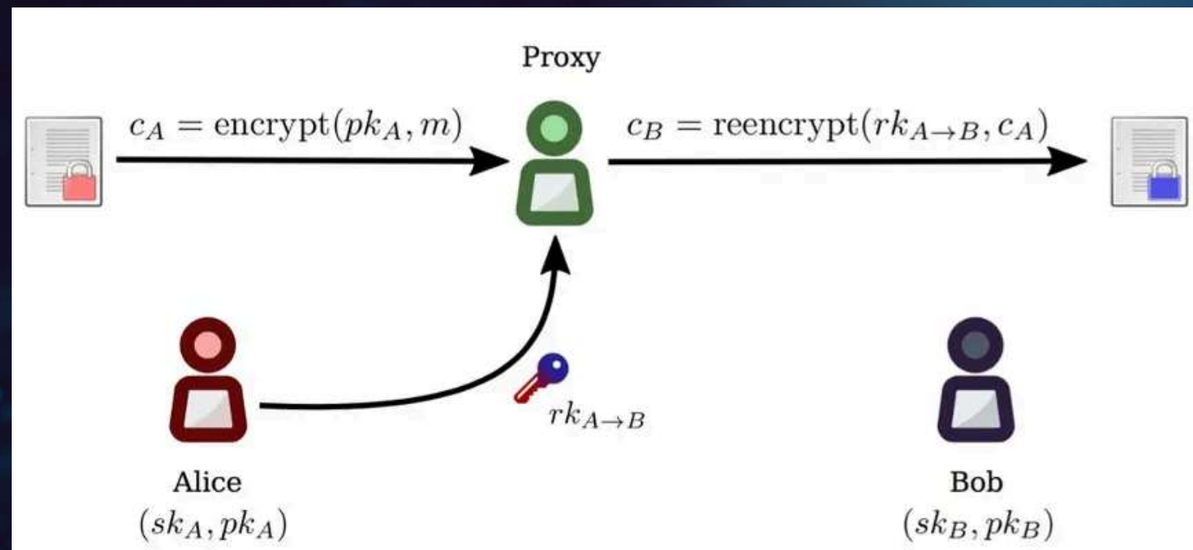
WHAT IS PROXY RE-ENCRYPTION (PRE)?

"Proxy re-encryption, or PRE, allows a third party — called the proxy — to convert a ciphertext encrypted under one person's public key, say Alice's, into a ciphertext that another person, Bob, can decrypt with his private key. Importantly, this is done without the proxy ever learning the underlying message."

REAL-WORLD PRE: ENCRYPTED EMAIL FORWARDING

Imagine Alice wants to temporarily forward her encrypted emails to Bob. Giving Bob her private key is a significant security risk, compromising all her past and future communications.

Instead, Alice generates a special **re-encryption key** using Bob's public key. This key is given to a trusted proxy service. The proxy then uses this key to convert Alice's encrypted emails into a format Bob can decrypt with his own private key. This ensures secure, temporary access without exposing Alice's sensitive secrets.



PRE IN ACTION: WALMART'S DATA ECOSYSTEM

Walmart manages vast amounts of user data, accessed by various departments like customer support, logistics, and fraud detection. My PRE model offers fine-grained, temporary access to encrypted customer data without ever exposing raw information or compromising encryption keys.

IMPACT & FUTURE COMPLIANCE

ENHANCED DATA SECURITY
PRE significantly elevates data security at scale, protecting sensitive user information from unauthorized access and breaches.

STREAMLINED DATA ACCESS
Departments can securely access the specific data they need, when they need it, fostering efficiency without sacrificing privacy.

REGULATORY COMPLIANCE
This solution inherently supports and simplifies adherence to stringent data privacy regulations like GDPR and CCPA.

FUTURE-PROOFING
By adopting PRE, organizations proactively prepare for evolving privacy demands and cryptographic advancements.