

ENCRYPTION



Our technology can be used for a wide variety of encryption tasks. Since it acts on encryption keys, it can be seamlessly layered on top of existing systems and avoids the need to directly use the base key received from NSA, ensuring it remains secure for an extended period. Tokens can be centrally manufactured, produced where needed with distributed equipment, or replaced with improvised tokens like car parts. Replacement policies and cycling times can also vary to meet the needs of the application, and users can securely adapt the system on the fly in response to developing circumstances.

A carrier strike group is an excellent example of how our technology can overcome extreme complexity. To maximize security, tokens would be replaced daily and new measurements taken every 10 minutes. This means the encryption key would change every 10 minutes without ever transmitting a key, so even an incredibly lucky guess would only give a few minutes of data. Tokens would be manufactured ashore and stored in tamper-evident containers like the one shown above until needed, and then thrown overboard after use. If the mission is extended, the carrier can make new randomly generated tokens in its machine shop to remain secure without receiving new cryptographic data. A separate emergency token would also be carried to generate one-time use keys to receive new cryptographic data for satellite communications.