एंड-टू-एंड एन्क्रिप्शन

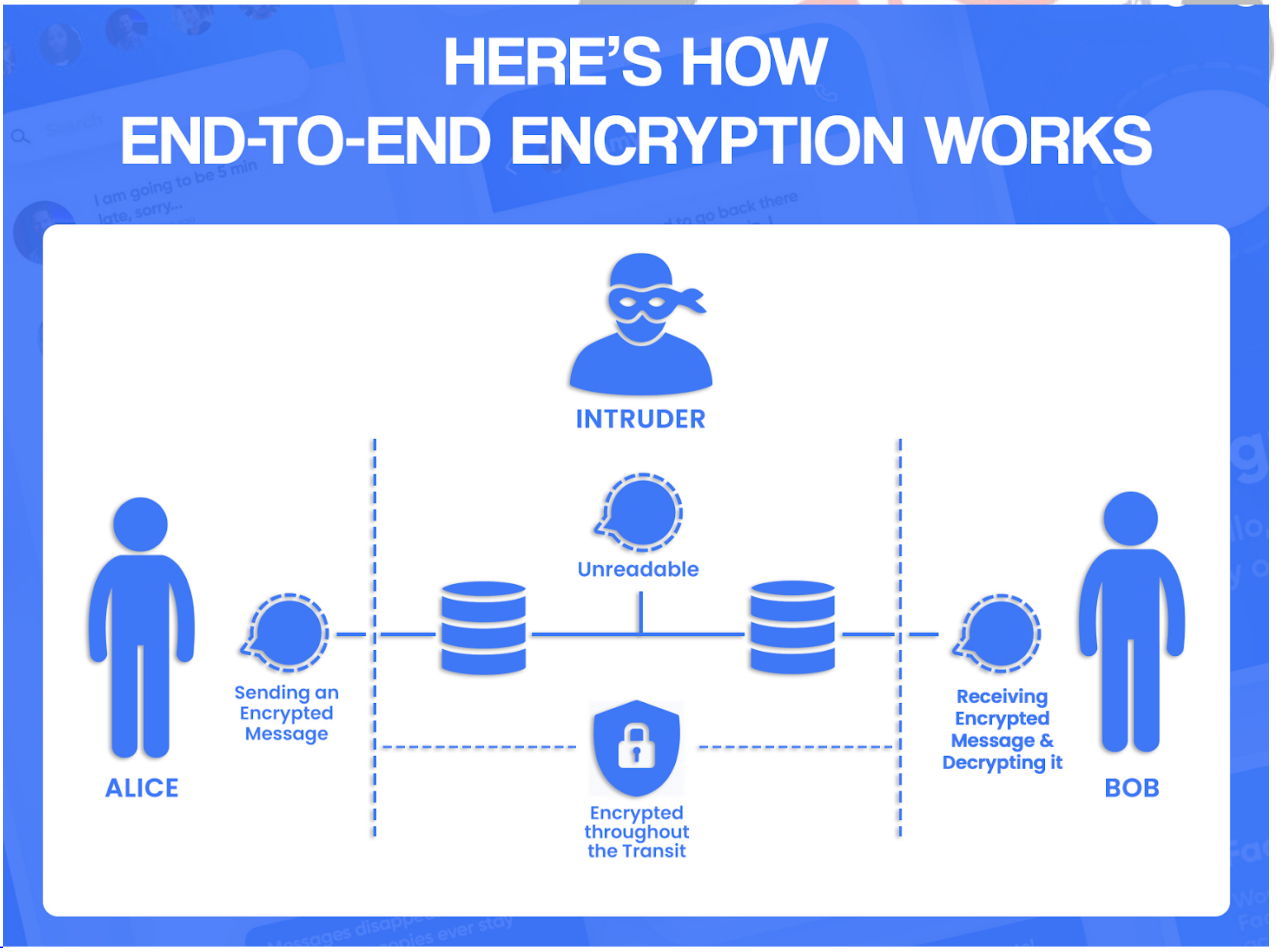
स्रोत: द हिंदू

एंड-टू-एंड एन्क्रिप्शन साइबर सुरक्षा के लिये महत्त्वपूर्ण है, जो प्रेषक और प्राप्तकर्त्ता दोनों के लिये विशेष रूप से **एन्कोडिंग** करके संवेदनशील डेटा का सुरक्षित प्रसारण सुनिश्चित करता है।

- यह विशेष रूप से बढ़ते साइबर हमलों या अनधिकृत पहुँच, चोरी, निगरानी और छेड़छाड़ से बचाता है।

एन्क्रिप्शन क्या है?

- **परिचय:**
  - एंड-टू-एंड एन्क्रिप्शन एक संचार प्रक्रिया है जो दो उपकरणों के बीच साझा किये जा रहे डेटा को एन्क्रिप्ट करती है।



//

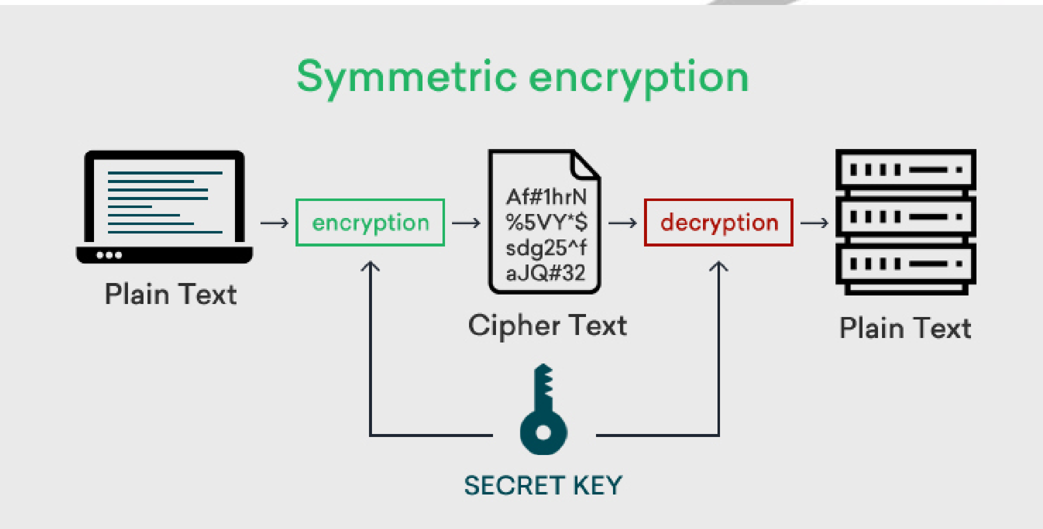
- **एंड-टू-एंड एन्क्रिप्शन:** E2E एन्क्रिप्शन में उन विशिष्ट बिंदुओं को सुरक्षित करना शामिल है जिनके माध्यम से डेटा प्रसारित किया जाता है।

- मैसेजिंग ऐप पर किसी मित्र के साथ संचार करते समय, अनधिकृत पहुँच को रोकने के लिये ट्रांज़िट के दौरान संदेशों को एन्क्रिप्ट किया जाता है, **एन्क्रिप्शन-इन-ट्रांज़िट दोनों** को नियोजित करना, जो सर्वर और उपयोगकर्त्ता के बीच रिले के दौरान संदेशों को सुरक्षित करता है एवं **एंड-टू-एंड एन्क्रिप्शन (E2E),** जो **ट्रांज़िट** के दौरान तथा सर्वर पर संग्रहीत होने तक एन्क्रिप्शन सुनिश्चित करता है जब तक कि कंटेनर इसे डिक्रिप्ट नहीं करता।

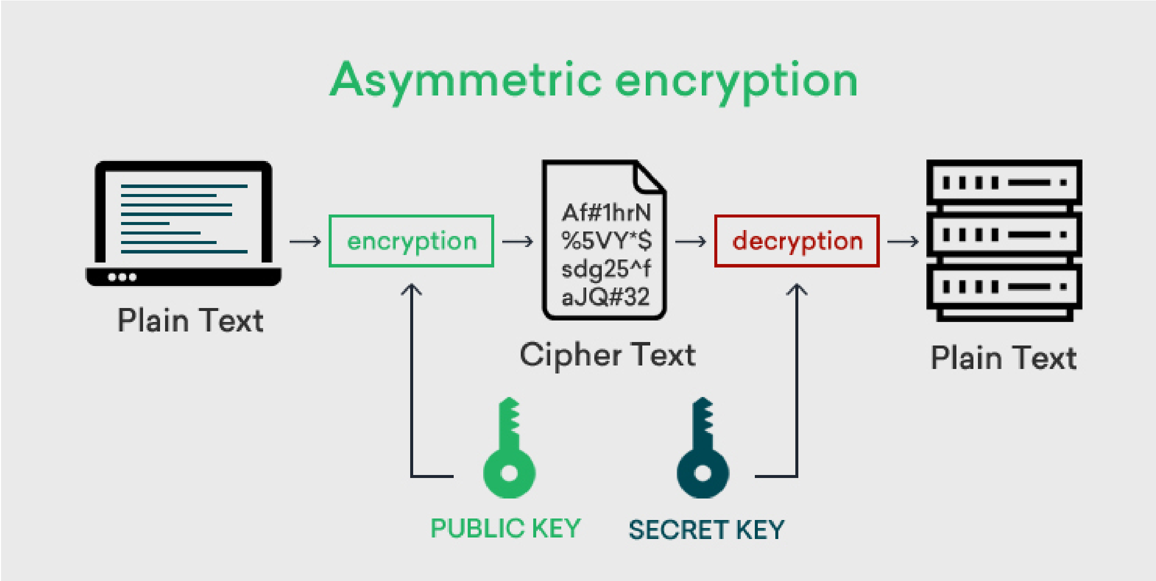
इसके बारे में इस तरह से सोचें:

- **नियमित संदेश:** पोस्टकार्ड भेजना - इसे कोई भी पढ़ सकता है।
- **एंड-टू-एंड एन्क्रिप्शन:** एक सीलबंद, कोडित अक्षर/शब्द भेजना - केवल सही कोड वाला प्राप्तकर्त्ता ही इसे पढ़ सकता है।

- **एन्क्रिप्शन की प्रक्रिया:** जानकारी के लिये गोपनीयता और सुरक्षा के वांछित स्तर के आधार पर विभिन्न एन्क्रिप्शन विधियों को नियोजित किया जा सकता है।
  - **सममित एन्क्रिप्शन (Symmetric Encryption)** में एन्क्रिप्टिंग और डिक्रिप्टिंग जानकारी दोनों के लिये एक ही कुंजी का उपयोग करना शामिल है, **डेटा एन्क्रिप्शन मानक (DES)** एक सममित एन्क्रिप्शन प्रोटोकॉल के प्रसिद्ध उदाहरण के रूप में कार्य करता है।
    - कंप्यूटर की हार्ड ड्राइव को एन्क्रिप्ट करने या **वाई-फाई पासवर्ड** सेट करने जैसे परिदृश्यों में उपयोग किये जाने वाले **उन्नत एन्क्रिप्शन स्टैंडर्ड (AES)** द्वारा उदाहरण दिया गया सममित एन्क्रिप्शन, तब लाभदायक साबित होता है जब प्रेषक और प्राप्तकर्त्ता एक ही प्रकार की संस्थाएँ होते हैं।



- **असममित एन्क्रिप्शन (Asymmetric Encryption)**, जिसे **सार्वजनिक-कुंजी क्रिप्टोग्राफी** के रूप में भी जाना जाता है, **यह कुंजी की एक जोड़ी** का उपयोग करने के सिद्धांत पर काम करता है: एक सार्वजनिक कुंजी और एक निजी कुंजी।
  - **पब्लिक की (Public Key)** सार्वजानिक तौर पर साझा की जाती है तथा संदेशों को एन्क्रिप्ट करने के लिये कोई भी इसका उपयोग कर सकता है किंतु केवल संबंधित **निजी/गुप्त कोड** का जानकार ही उन संदेशों को डिक्रिप्ट कर सकता है।
  - यह असममित एन्क्रिप्शन दृष्टिकोण दोनों पक्षों को एक ही कुंजी साझा करने की आवश्यकता के बिना **सुरक्षित संचार सुनिश्चित करता है।** इस प्रकार एन्क्रिप्शन प्रक्रिया भले ही सार्वजनिक हो सकती है किंतु डिक्रिप्शन निजी रहता है जो संचार का एक सुरक्षित साधन प्रदान करता है।



- **E2E एन्क्रिप्शन की कमियाँ:** हालाँकि E2E एन्क्रिप्शन एक सुदृढ़ सुरक्षा उपाय है किंतु [मैन इन द मिडिल (MITM) हमलों](), उपयोगकर्त्ता की संतुष्टि, मैलवेयर खतरों, कंपनी के विगत मामले तथा कानूनी आवश्यकताओं जैसे संभावित कारक, एन्क्रिप्टेड संदेश की समग्र सुरक्षा को प्रभावित कर सकते हैं।

हैश फंक्शन की क्या भूमिका है?

- विभिन्न तरीकों से सन्देश को एन्क्रिप्ट करने के लिये विभिन्न सममित तथा असममित प्रणालियों द्वारा विभिन्न [हैश फंक्शन]() का उपयोग किया जाता है।
    - हैश फंक्शन की भूमिका कुछ गुणों को सुनिश्चित करते हुए एक संदेश को एन्क्रिप्ट करना है:
        - **संदेश छिपाना:** हैश फंक्शन किसी इनपुट संदेश का **एन्क्रिप्टेड संस्करण** तैयार करता है जिसे **डाइजेस्ट** के रूप में जाना जाता है। डाइजेस्ट शब्द को सार्थकता प्रदान करते हुए यह मूल संदेश की गोपनीयता को बनाए रखता है।
        - **फिक्स्ड लेंथ आउटपुट:** फंक्शन विभिन्न आकार के संदेशों को एक प्रभावी डाइजेस्ट में परिवर्तित करता है। इस कारण मूल संदेश की लंबाई का **डाइजेस्ट लेंथ** की तुलना में लंबाई का अनुमान लगाना कठिन हो जाता है।
        - **विशिष्ट डाइजेस्ट:** हैश फंक्शन का कार्य अद्वितीय संदेशों के लिये अद्वितीय डाइजेस्ट का उत्पादन करना है, यह सुनिश्चित करते हुए कि विभिन्न संदेशों का परिणाम एक ही **हैश** में न हो।

UPSC सिविल सेवा परीक्षा, विगत वर्ष के प्रश्न

⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰:

प्रश्न. 'वान्नाक्राई, पेट्या और इटरनलब्लू' पद जो हाल ही में समाचारों में उल्लिखित थे, निम्नलिखित में से किसके साथ संबंधित हैं ?

(a) एक्सोप्लैनेट्स
(b) प्रच्छन्न मुद्रा (क्रिप्टोकरेंसी)
(c)साइबर आक्रमण
(d) लघु उपग्रह

उत्तर: (c)

⍰⍰⍰⍰⍰⍰:

प्रश्न. भारत की आतंरिक सुरक्षा को ध्यान में रखते हुए, सीमा-पार से होने वाले साइबर हमलों के प्रभाव का विश्लेषण कीजिये । साथ ही, इन परिष्कृत हमलों के विरुद्ध रक्षात्मक उपायों की चर्चा कीजिये। (2021)

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/end-to-end-encryption-2