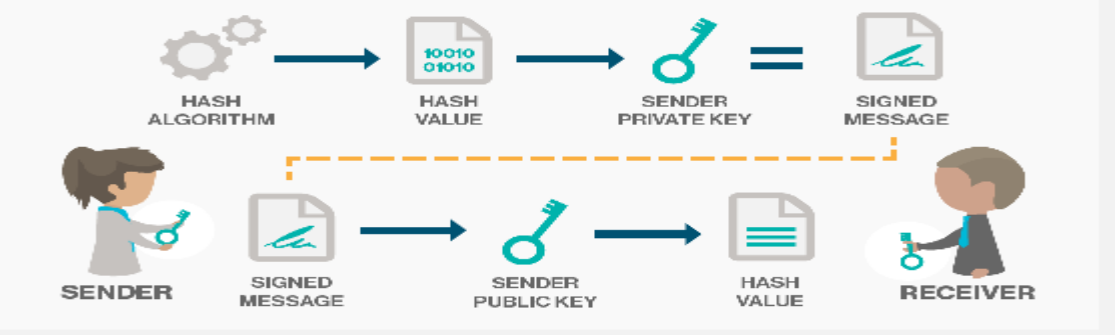
डिजिटल सिग्नेचर

DIGI PAGE

Subject - Computer

Date of Release - 05-NOV-2017

डिजिटल हस्ताक्षर या सिग्नेचर एक प्रकार का कंप्यूटर कोड होता है, इसका प्रयोग केवल अधिक्रत व्यक्ति ही कर सकता है, जिसे उपयोग करने के लिये या तो यूजर आईडी और पासवर्ड की आवश्यकता होती है, इसके अलावा कहीं-कहीं डोंगल का भी प्रयोग किया जाता है जो एक प्रकार की पेनड्राइव जैसी डिवाइस होती है, यानि डिजिटल सिग्नेचर केवल वही व्यक्ति कर पायेगा, जिसके पास यह दोनों चीजें हों। जैसे कागज के सर्टिफिकेट्स पर मैनुअली साइन किये जाते थे, वैसे ही इलैक्ट्रोनिक सर्टिफिकेट्स पर डिजिटल सिग्नेचर किये जाते हैं। यह कानूनी तौर पर मान्य होते हैं।



Digital Signature Public key Cryptogrphy के ऊपर ही आधारित है जिसे Asymmetric Cryptography भी कहते हैं. ये Public key Algorithm जैसे की RSA का इस्तमाल कर के दो keys generate करता है जो की हैं Private और Public. और ये दोनों keys Mathematically linked होते हैं. Digital Signature बनाने के लिए Signing Software की मदद से जिस electronic data का signature बनाना है उसका one way Hash बनाया जाता है. फिर Private Key की मदद से hash को encrypt किया जाता है. इसी encrypted hash और उसके संग जुड़े दुसरे information जैसे Hashing Algorithm को Digital Signature कहा जाता है.

यहाँ हम पूरे message की जगह खाली Hash को ही encrypt करते हैं ऐसा इसलिए क्यूंकि Hash Function की मदद से हम किसी arbitrary input को एक fixed length value में तब्दील कर सकते हैं जो की आम तोर से छोटा होता है. इससे समय की बचत होती है क्यूंकि Hashing, Signing के मुकाबले बहुत faster है.

और अधिक ऑनलाइन परीक्षा का अभ्यास करने के लिए जाएँ: https://myshop.mahendras.org