md5 Encrypt

L' **MD5 Message-Digest Algorithm** è ampiamente utilizzato funzione crittografica di hash che produce una 128 - bit (16 byte), valore hash. Specificato in RFC 1321, MD5 è stato impiegato in una vasta gamma di applicazioni di sicurezza, e viene anche comunemente utilizzata per verificare l'integrità dei dati. Tuttavia, è stato dimostrato che MD5 non è collisione resistente; [3] in quanto tali, MD5 non è adatto per applicazioni come SSL certificati o firme digitali che si basano su questa proprietà. Un hash MD5 viene generalmente espresso in 32 cifre esadecimali numero.

MD5 è stato progettato da Ron Rivest nel 1991 per sostituire una funzione di hash in precedenza, MD4. Nel 1996, un difetto è stato trovato con la progettazione di MD5. Anche se non era chiaramente una debolezza fatale, crittografi iniziato raccomandare l'uso di altri algoritmi, come SHA-1 (che da allora è stata trovata anche di essere vulnerabili). Nel 2004, i difetti più gravi sono stati scoperti, facendo un ulteriore uso degli algoritmi per motivi di sicurezza discutibili, in particolare, un gruppo di ricercatori hanno descritto come creare un paio di file che condividono lo stesso MD5 checksum. [4]

[5]

Ulteriori progressi sono stati made in rottura MD5 nel 2005, 2006 e 2007. [6]

In un attacco contro MD5 pubblicato nel dicembre 2008, un gruppo di ricercatori hanno usato questa tecnica per falso validità del certificato SSL. [7] [8]

US-CERT afferma MD5 "deve essere considerato crittograficamente rotto e non idonei per un ulteriore uso," [9] e la maggior parte delle applicazioni governo degli Stati Uniti ora richiedono l' SHA-2 famiglia di funzioni hash. [10]

Enter your text to encrypt :

(This is usually a password eg. yellow32)

//