**UNIVERSIDADE DO EXTREMO SUL CATARINENSE - UNESC**

**CURSO DE CIÊNCIA DA COMPUTAÇÃO**

**GUILHERME WALTRICKE FREITAS**

**PAULO HENRIQUE MACHADO GALATTO**

**CRIPTOGRAFIA UTILIZANDO MD5**

**CRICÍUMA**

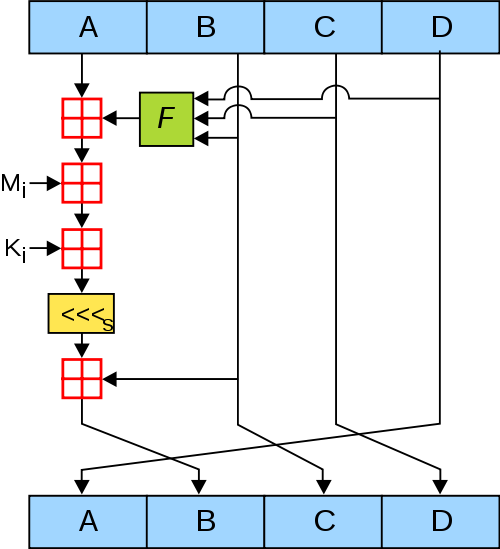
**2014**

MD5 Message-Digest Algorithm tem sido mundialmente utilizado como um gerador de criptografia em hash, produzindo 128-bit (16 bytes), o código hash gerado pelo MD5 é transformado em uma string com 32 dígitos no formato hexadecimal.

Algoritmo criado por Ron Rivest em 1991 para substituir o defasado MD4. O código do algoritmo foi publicado em uma RFC de número 1321 com a atribuição a RSA License.

Em meados de 1996 uma falha foi descoberta na estrutura lógica do código, enquanto esta falha não se espalhou como uma fraqueza, pesquisadores começaram a recomendar o uso de outros algoritmos como o SHA-1 que também desde um tempo após também foi identificado com vulnerabilidades. No inicio de 2004 foi provado que o MD5 não possuía resistência a ataques de colisão, diante deste fato o algoritmo criado por Rivest não poderia mais ser utilizado em certificados SSL ou assinaturas digitais. Também em 2004, mais no fim dele, pesquisadores conseguiram explorar uma falha com maior impacto, os mesmos criaram pares de arquivos diferentes que compartilhavam o mesmo hash MD5, sendo assim quebrando a ideologia do checksum, a partir disto outras falhas foram ainda mais exploradas nos anos seguintes: 2005, 2006 e 2007. O Governo americano declarou que o MD5 deveria ser considerado uma técnica de criptografia quebrada e que deveria ser banida do uso por motivos de seguranças futuros, sendo assim o governo iniciou a certificar apenas aplicações que rodem o SHA-2 como gerador de hash.

O Funcionamento do algoritmo de MD5 é baseado em um fixado processamento e tamanho de saída do hash, ou seja, independente do tamanho do texto original o hash sempre terá um mesmo tamanho fixo. Quando o algoritmo recebe um texto a ser criptografado, ele quebra a mensagem em 4 blocos de 512-bit (A,B,C e D), a partir desta quebra ele se utiliza de mudanças e substituições de bits, se apropriando de cálculos com base em operações de máquinas como AND, OR, NOT e XOR. A imagem abaixo mostra o design do funcionamento do algoritmo.



Importante salientar que uma vez que um texto é transformado em hash pelo algoritmo é impossível voltar a sua mensagem original.

**REFERÊNCIAS**

WIKIPEDIA, MD5Sum em 2014, Disponível em: http://en.wikipedia.org/wiki/Md5sum>. Acesso em: 14 maio 2014.

PHP Documentation, MD5 Hash em 2014, Disponível em: http://www.php.net/manual/en/function.md5.php>. Acesso em: 14 maio 2014.

WIKIPEDIA, MD5 em 2014, Disponível em: http://en.wikipedia.org/wiki/MD5>. Acesso em: 14 maio 2014.

CODEPROJECT, MD5 Hash SQL Server Extended Stored Procedure em 2014, Disponível em: http://www.codeproject.com/Articles/5963/MD-Hash-SQL-Server-Extended-Stored-Procedure>. Acesso em: 13 maio 2014.