**Wie läuft die Verschlüsselung?**

-SHA-512 (sicherer Hash-Algorithmus) liefert immer einen verschlüsselten Hex-String mit genau 128 Zeichen zurück ,wir speichern das 128-stellige Passwort in der Datenbank und verschlüsseln das eingegebene Passwort des Benutzers. Dann vergleichen wir beide. Wenn Sie gleich sind, können wir davon ausgehen, dass das richtige Passwort gewählt wurde.

**Warum SHA-512?**

- Es wird immer ein 128-stellige Passwort gespeichert egal, wie lang das Passwort war.

-Tatsächlich sind Kollisionen(=gleiche Verschlüsselung bei ungleichem Klartext) bei SHA-512 extrem selten.

**Warum nicht andere Methode?**

-Die bekanntesten Verfahren sind MD5 ,MD4 und SHA1 extrem unsicher ,sind inzwischen ziemlich einfach zu knacken.

-Ceaser-Chiffre oder das Enigma-Chiffre haben das Problem, dass zumindest ersteres selbst von Hand schnell geknackt ist, und dass jeder z.B. die Länge des Passwortes selbst an der verschlüsselten Form sehen kann.