

# php to perl translation

---

*Source:* <http://coding.derkeiler.com/Archive/Perl/perl.beginners/2007-06/msg00471.html>

---

- *From:* [andreas.moroder@xxxxxxxxxxxxx](mailto:andreas.moroder@xxxxxxxxxxxxx) (Andreas Moroder)
  - *Date:* Mon, 18 Jun 2007 10:55:17 +0200
- 

Hello,

after a long search I found a script that creates oracle password hashes. I need the result of this script to store the password in out LDAP database in the oracle hashed format. The problem is that it is a php script and I need it in perl.

I am a perl beginner and I am not able to convert this script to perl.  
Is anyone outthere that could help me ?

Passing user=scott and password=tiger

the result of the function should be.

F894844C34402B67

The mcrypt functions should be used.

Thank you very much  
Andreas

```
<?php
$username = "scott";
$password = "tiger";

// Using thirdparty library for DES with CBC encryption
echo get_oracle_hash($username, $password, $use_mcrypt=false);

echo "<br/>";

// Using built-in mcrypt library for encryption
echo get_oracle_hash($username, $password, $use_mcrypt=true);

/*
```

## ORACLE HASH ALGORITHM

1. Concatenate the username and the password to produce a plaintext string;
2. Convert the plaintext string to uppercase characters;
3. Convert the plaintext string to multi-byte storage format; ASCII characters have the high byte set to 0x00;
4. Encrypt the plaintext string (padded with 0s if necessary to the next even block length) using the DES algorithm in cipher block chaining (CBC) mode with a fixed key value of 0x0123456789ABCDEF;
5. Encrypt the plaintext string again with DES-CBC, but using the last block of the output of the previous step (ignoring parity bits) as the encryption key. The last block of the output is converted into a printable string to produce the password hash value.

```
*/  
// $username: The user name  
// $password: The password for the user  
// $use_mcrypt: If we want to use built in library mcrypt (need to set server php settings)  
function get_oracle_hash($username, $password, $use_mcrypt=true)  
{  
    // Want to use mcrypt  
    if ($use_mcrypt)  
    {  
        // Values if we want to use mcrypt library  
        $cipher = MCRYPT_3DES;  
        $mode = MCRYPT_MODE_CBC;  
    }  
    // Want to use thirdparty library  
    else  
    {  
        require_once("DesCbc.php");  
    }  
  
    // The data we want to encrypt/make hash of  
    // We have to convert it to multibyte format  
    $temp_data = strtoupper($username) . strtoupper($password);  
    $data = "";  
    foreach (str_split($temp_data) as $char)  
    {  
        // High byte: 0x00, (i.e. H = 0x0048)  
        $temp_hex = "00" . dechex(ord($char));  
  
        // Have to handle some special characters different  
        if (in_array($char, str_split(&
```