Securitatea în MySQL

Criptarea

- Criptografia este ştiinţa care foloseşte matematica pentru a cripta şi decripta informaţii; cu alte cuvinte, pentru a securiza informaţiile stocate ori transmise.
- Reversul medaliei este *criptanaliza* - ştiinţa analizării şi spargerii codurilor prin care se codifică datele.
- Cele două, criptografia şi criptanaliza sunt denumite generic *criptologie*.

Criptarea

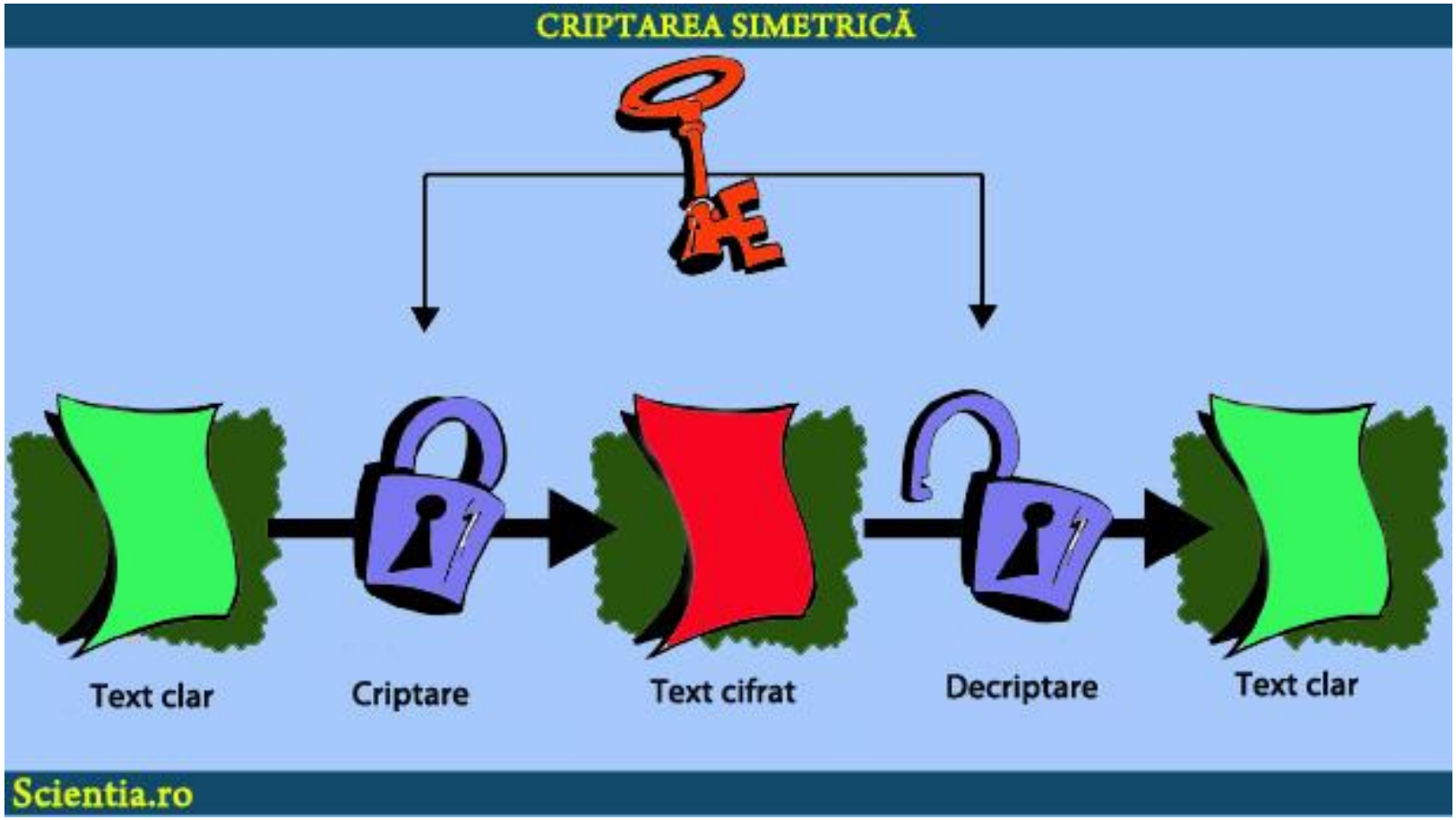
- *Criptarea* se face cu ajutorul unui algoritm şi a unei chei de criptare.
- *Algoritmul* este o funcţie matematică folosită efectiv în procesul de criptare şi decriptare.
- Combinarea algoritmului cu o anume *cheie de criptare* dă un rezultat diferit de combinarea aceluiaşi algoritm cu o altă cheie de criptare.
- *Tăria criptării* depinde atât de *tăria algoritmului*, cât şi de *tăria cheii de criptare*.
- În urma criptării, informaţiile devin indescifrabile; fără a avea cheia cu care s-a efectuat criptarea, decriptarea este imposibilă (sau cel puţin aşa se vrea).

Criptarea

- Criptarea este de două feluri:
  - criptarea simetrică
  - criptarea asimetrică (criptarea cu cheie publică)

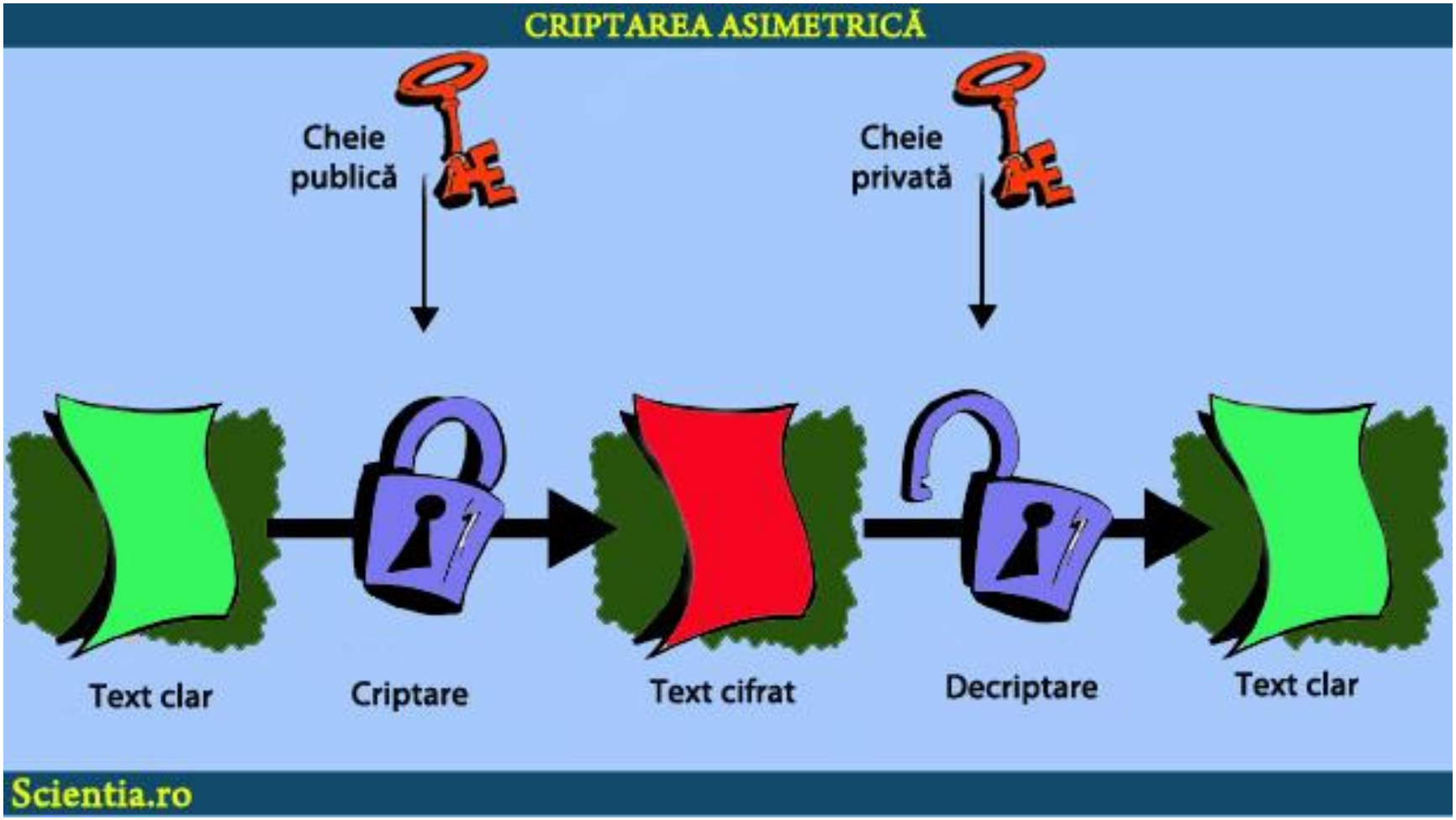
Criptarea simetrică

- *Pe un computer se realizează criptarea informaţiilor cu ajutorul unui algoritm şi o anume cheie*.
- *Apoi, informaţia criptată pleacă (fără măsuri de protecţie specială) către destinatar.*
- *Destinatarul va vedea informaţia în clar, o va putea decodifica, doar dacă are cheia corespondentă. Dacă o are, o aplică fişierului criptat şi are astfel acces la informaţie în clar.*


CRIPTAREA SIMETRICĂ
Text clar
Criptare
Text cifrat
Decriptare
Text clar
Scientia.ro

Criptarea asimetrică

- *Criptografia cu cheie publică* funcţionează în felul următor: se foloseşte o cheie publică, care nu este secretă, pentru criptare, şi o cheie privată pentru decriptare.
- Cu alte cuvinte, *oricine poate cripta cu o cheie publică*, dar *numai cel care are cheia privată poate decripta*.


CRIPTAREA ASIMETRICĂ
Cheie publică
Cheie privată
Text clar
Criptare
Text cifrat
Decriptare
Text clar
Scientia.ro

AES_ENCRYPT și AES_DECRYPT

- Permit criptarea/decriptarea simetrică folosind algoritmul AES (Advanced Encryption Standard)
- Este folosit criptarea cu o cheie de 128 biți (poate fi mărit pînă la 256 biți)

Sintaxa

- AES_ENCRYPT(str,key_str)
- AES_DECRYPT(crypt_str,key_str)

- Str șirul de caractere care trebuie criptat
- key_str – cheia secretă

- Dacă unul din argumente este Null, atunci și rezultatul este Null

Exemplu

```
mysql> SELECT AES_ENCRYPT('MySQL','секретный ключ');
+----------------------------------------+
| AES_ENCRYPT('MySQL','секретный ключ')  |
+----------------------------------------+
| ...ЗАьZЭj9к•-еП™МЋ                     |
+----------------------------------------+
mysql> SELECT AES_DECRYPT('...ЗАьZЭj9к•-еП™МЋ','секретный ключ');
+-------------------------------------------------+
| AES_DECRYPT('...ЗАьZЭj9к•-еП™МЋ','секретный ключ') |
+-------------------------------------------------+
| MySQL                                           |
+-------------------------------------------------+
```

Exemplu

```
mysql> SELECT email FROM users;
```

```
+-------------------------+
| email                   |
+-------------------------+
| ivanov@email.ru         |
| losev@email.ru          |
| simdyanov@softtime.ru   |
| kuznetsov@softtime.ru   |
| NULL                    |
| korneev@domen.ru        |
+-------------------------+
```

```
mysql> UPDATE users SET email = AES_ENCRYPT(email,'Бызэ даннух');
mysql> SELECT email FROM users;
+------------------------------------+
| email                              |
+------------------------------------+
| □хтЫl—lЬ}'.r@™Ц                    |
| №.LЙтъўЕ□ѓ¦ФUIЪ«н                  |
| ЂIgПуLA □2W□TI,,jeE:rУ@ддS
пСгц·  |
| =-"рО26ецЩгу□jeE:rУ@ддS
пСгц·  |
| NULL                               |
Vl' |ЂчўЧ_ПLЌЕЩ•БМ...ътЬ©л»пж¬□я
+------------------------------------+
```

```
mysql> SELECT AES_DECRYPT(email,'бызэ даннух') FROM users;
+-------------------------------------+
| AES_DECRYPT(email,'бызэ даннух') |
+-------------------------------------+
| ivanov@email.ru                     |
| losev@email.ru                      |
| simdyanov@softtime.ru               |
| kuznetsov@softtime.ru               |
| NULL                                |
| korneev@domen.ru                    |
+-------------------------------------+
```

Funcțiile ENCODE și DECODE

- ENCODE(str,pass_str)
- DECODE(crypt_str,pass_str)

Funcțiile DES_ENCRYPT și DES_DECRYPT

- Permit criptarea simetrică cu ajutorul algoritmului 3DES (Triple-DES)

- DES_ENCRYPT(string_to_encrypt [, (key_number | key_string)])
- DES_DECRYPT(string_to_decrypt [, key_string])

Argumente

- string_to_encrypt - șirul de caractere care trebuie criptat
- key_string - șir de caractere, opțional, indică cheia secretă. Dacă cheia s-a indicat la criptare, atunci ea trebuie folosită și la decriptare.
- În loc de cheia secretă poate fi indicat key_number (ia valori de la 0 la 9) indică numărul liniei în fișierul DES de pe server, localizarea căruia este indicată la pornirea serverului MySQL prin --des-key-file. Pentru funcția DES_DECRYPT() deja nu este necesar de a indica acest parametru.

Funcția ENCRYPT

- Permite criptarea ireversibilă
- Se apelează funcția de sistem crypt() (UNIX)
- ENCRYPT(str [, salt])
  - Str - șirul de caractere care va fi criptat, decriptarea lui ulterioară nu va fi posibilă
  - Salt – parametru opțional, dacă lipsește, rezultatul criptării va fi de fiecare dată diferit

Exemplu

```
mysql> SELECT ENCRYPT('MySQL'), ENCRYPT('MySQL');
+--------------------+--------------------+
| ENCRYPT('MySQL')   | ENCRYPT('MySQL')   |
+--------------------+--------------------+
| qnhlAW/pwGY2A      | snshG/AgkhKoU      |
+--------------------+--------------------+
```

```
mysql> SELECT ENCRYPT('MySQL','password'), ENCRYPT('MySQL','password');
+--------------------------------+--------------------------------+
| ENCRYPT('MySQL','password')    | ENCRYPT('MySQL','password')    |
+--------------------------------+--------------------------------+
| pa6Fh2dhjP10c                  | pa6Fh2dhjP10c                  |
+--------------------------------+--------------------------------+
```

Funcția MD5

- Permite criptarea ireversibilă după algoritmul MD5 (Message-Digest Algorithm)
- Sintaxa: MD5(str)
- Funcția primește un singur parametru – str - șir de caractere și returnează o sumă de control pe 128 biți determinată după algoritmul MD5. Valoarea returnată este un număr hexazecimal, unic pentru șir.

```
mysql> SELECT MD5('MySQL'), MD5('MySQL');
+----------------------------------+----------------------------------+
| MD5('MySQL')                     | MD5('MySQL')                     |
+----------------------------------+----------------------------------+
| 62a004b95946bb97541afa471dcca73a | 62a004b95946bb97541afa471dcca73a |
+----------------------------------+----------------------------------+
mysql> SELECT MD5('MySQL1'), MD5('MySQL');
+----------------------------------+----------------------------------+
| MD5('MySQL1')                    | MD5('MySQL')                     |
+----------------------------------+----------------------------------+
| fc3dd4ddcb132de1f9552818344e1b09 | 62a004b95946bb97541afa471dcca73a |
+----------------------------------+----------------------------------+
```

Funcția PASSWORD

- Permite criptarea ireversibilă a unui șir str:
- PASSWORD(str)
- Această funcție este folosită de MySQL pentru criptarea parolei în cîmpul password din tabelul user

Exemplu

```
mysql> SELECT PASSWORD('MySQL');
+-------------------------------------------+
| PASSWORD('MySQL')                         |
+-------------------------------------------+
| *1799AB5202FE2E9958365F9B3ECBBF53657254C7 |
+-------------------------------------------+
```

```
mysql> SELECT PASSWORD('MySQL'), OLD_PASSWORD('MySQL');
+-------------------------------------------+----------------------+
| PASSWORD('MySQL')                         | OLD_PASSWORD('MySQL') |
+-------------------------------------------+----------------------+
| *1799AB5202FE2E9958365F9B3ECBBF53657254C7 | 7c651ebc23eebf89      |
+-------------------------------------------+----------------------+
```

Funcția SHA1

- Determină suma de control pe 160 biți după algoritmul SHA1 (Secure Hash Algorithm) pentru șirul str:
- SHA1(str)
- Returnează un număr hexazecimal (40 cifre) sau Null.

Exemplu

```
mysql> SELECT SHA('MySQL');
+------------------------------------------+
| SHA('MySQL')                             |
+------------------------------------------+
| deaa0c393a6613972aaccbf1fecfdad67aa21e88 |
+------------------------------------------+
```