
CTF
TIME

Разбор первой задачи

- QR – код
- Base 64
- Google: brute force
- png

QR-код

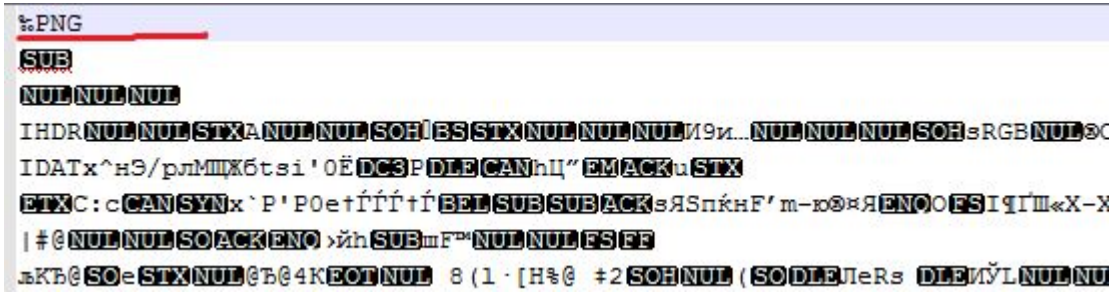
Base 64

- Позиционная система счисления с основанием 64.
- Широко используется в электронной почте для представления бинарных файлов в тексте письма.
- На каждые 3 байта данных приходится 4 символа.

Brute force

Сигнатура файла

- Набор байтов, обеспечивающий идентификацию типа файла.
- В Linux: команда file
- В Windows: FileType Verificator



Стеганография

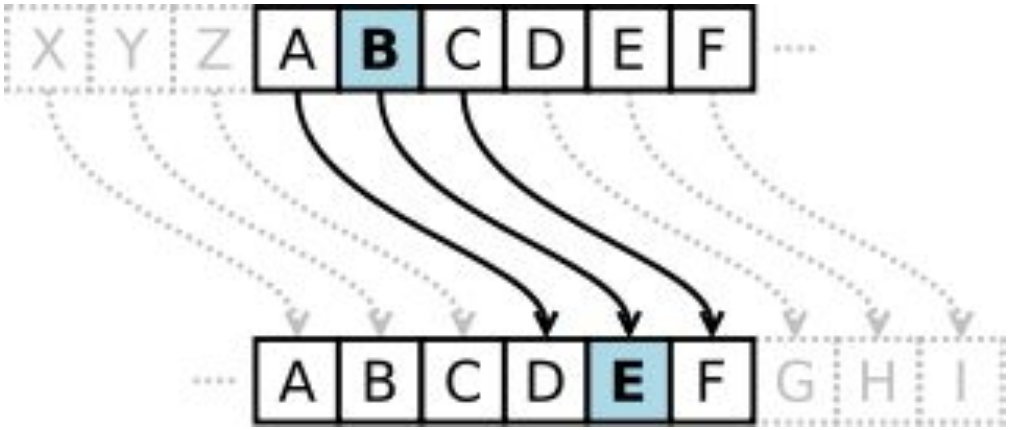
- Это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи.

Криптография

- Наука о шифровании
- Некоторые виды шифрования:
  - классическое шифрование
  - продвинутые шифры
  - хеш-функции

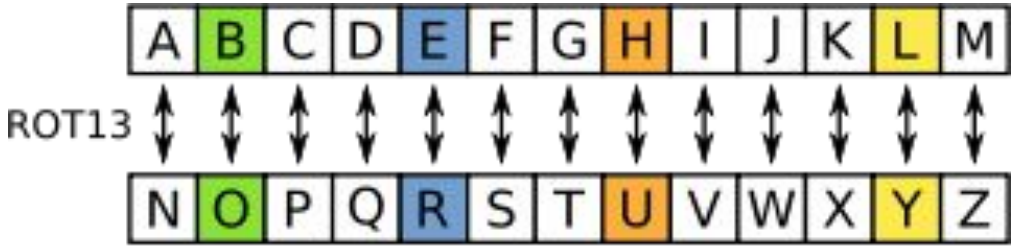
Scytale

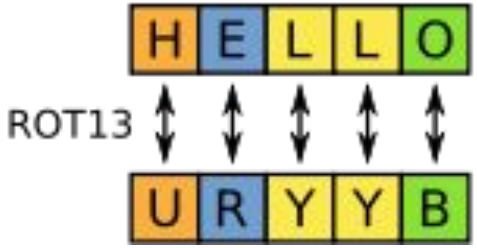
Caesar



ROT13

- Тот же шифр Цезаря





XOR

Hill cipher

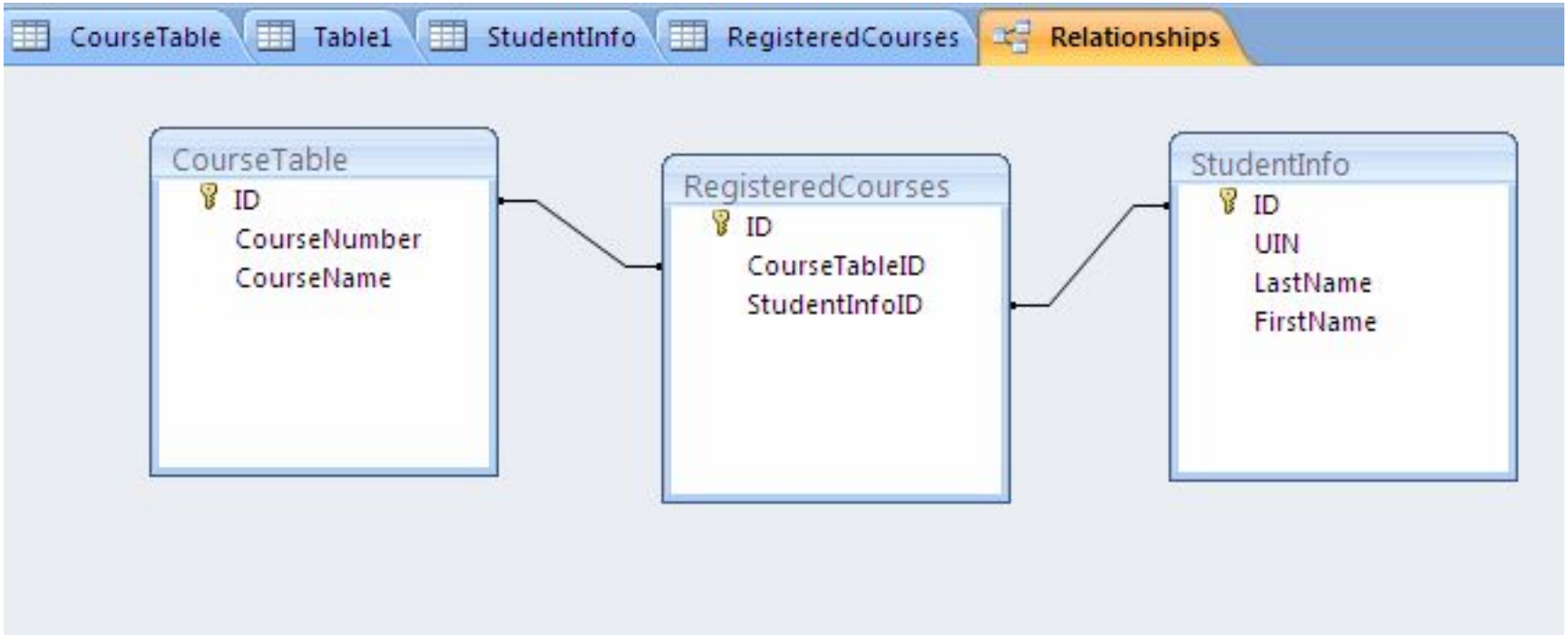
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 3 \\ 14 \\ 6 \end{pmatrix} = \begin{pmatrix} 360 \\ 323 \\ 388 \end{pmatrix} \equiv \begin{pmatrix} 22 \\ 11 \\ 24 \end{pmatrix} \pmod{26}$$

SQL

- Язык программирования, применяемый для создания, модификации и управления данными в произвольной реляционной базе данных.

Реляционная база данных



Получить данные из таблицы

```
SELECT secret
FROM t_users
WHERE
id=1
AND
password = ‘gnom';
```

Что происходит на сервере

```php
if(isset($_GET['id'])) {
  $id = $_GET['id'];
  $sql = 'SELECT id, flag FROM secret WHERE id = '.$id;
  $result = mysql_query($sql);
}
```