变异凯撒（实验吧CTF题库-密码学）

原创

皮卡皮卡~ 于 2019-05-21 08:49:18 发布 7195 收藏 19

分类专栏： CTF题库 文章标签： 凯撒加密 CTF 密码学 变异凯撒

本文链接：https://blog.csdn.net/y_universe/article/details/90376962

CTF题库 专栏收录该内容

10 篇文章 5 订阅

订阅专栏

变异凯撒（实验吧CTF题库-密码学）

题目概述

分值：10 难度：易 解题通过率：92%

加密密文：`afZ_r9VYfScOeO_UL^RWUc`

格式：flag{}

题目链接：http://www.shiyanbar.com/ctf/2038

基础知识

根据题目名称“变异凯撒”可以推断这个题应该是用了凯撒加密的变异形式。

我们先来了解一下凯撒加密：

> 在密码学中，凯撒密码（英语：Caesar cipher），或称凯撒加密、凯撒变换、变换加密，是一种最简单且最广为人知的加密技术。它是一种替换加密的技术，明文中的所有字母都在字母表上向后（或向前）按照一个固定数目进行偏移后被替换成密文。例如，当偏移量是3的时候，所有的字母A将被替换成D，B变成E，以此类推。这个加密方法是以罗马共和时期凯撒的名字命名的，当年凯撒曾用此方法与其将军们进行联系。
>
> 恺撒密码通常被作为其他更复杂的加密方法中的一个步骤，例如维吉尼亚密码。恺撒密码还在现代的ROT13系统中被应用。但是和所有的利用字母表进行替换的加密技术一样，恺撒密码非常容易被破解，而且在实际应用中也无法保证通信安全。

参考解题步骤

1、观察密文，`afZ_r9VYfScOeO_UL^RWUc`

由于密文中有下划线和阿拉伯数字，所以推测应该不是用的字母表进行的替换加密，很有可能是用的ASCII码表。

ASCII表

(American Standard Code for Information Interchange 美国标准信息交换代码)

高四位 / 低四位		ASCII控制字符 0000 0						ASCII控制字符 0001 1						ASCII打印字符 0010 2		ASCII打印字符 0011 3		ASCII打印字符 0100 4		ASCII打印字符 0101 5		ASCII打印字符 0110 6		ASCII打印字符 0111 7		
		十进制	字符	Ctrl	代码	转义字符	字符解释	十进制	字符	Ctrl	代码	转义字符	字符解释	十进制	字符	十进制	字符	十进制	字符	十进制	字符	十进制	字符	十进制	字符	Ctrl
0000	0	0		^@	NUL	\0	空字符	16	▶	^P	DLE		数据链路转义	32		48	0	64	@	80	P	96	`	112	p	
0001	1	1	☺	^A	SOH		标题开始	17	◀	^Q	DC1		设备控制 1	33	!	49	1	65	A	81	Q	97	a	113	q	
0010	2	2	☻	^B	STX		正文开始	18	↕	^R	DC2		设备控制 2	34	"	50	2	66	B	82	R	98	b	114	r	
0011	3	3	♥	^C	ETX		正文结束	19	‼	^S	DC3		设备控制 3	35	#	51	3	67	C	83	S	99	c	115	s	
0100	4	4	♦	^D	EOT		传输结束	20	¶	^T	DC4		设备控制 4	36	$	52	4	68	D	84	T	100	d	116	t	
0101	5	5	♣	^E	ENQ		查询	21	§	^U	NAK		否定应答	37	%	53	5	69	E	85	U	101	e	117	u	
0110	6	6	♠	^F	ACK		肯定应答	22	▬	^V	SYN		同步空闲	38	&	54	6	70	F	86	V	102	f	118	v	
0111	7	7	•	^G	BEL	\a	响铃	23	↨	^W	ETB		传输块结束	39	'	55	7	71	G	87	W	103	g	119	w	
1000	8	8	◘	^H	BS	\b	退格	24	↑	^X	CAN		取消	40	(	56	8	72	H	88	X	104	h	120	x	
1001	9	9	○	^I	HT	\t	横向制表	25	↓	^Y	EM		介质结束	41	)	57	9	73	I	89	Y	105	i	121	y	
1010	A	10	◙	^J	LF	\n	换行	26	→	^Z	SUB		替代	42	*	58	:	74	J	90	Z	106	j	122	z	
1011	B	11	♂	^K	VT	\v	纵向制表	27	←	^[	ESC	\e	溢出	43	+	59	;	75	K	91	[	107	k	123	{	
1100	C	12	♀	^L	FF	\f	换页	28	∟	^\	FS		文件分隔符	44	,	60	<	76	L	92	\	108	l	124	|	
1101	D	13	♪	^M	CR	\r	回车	29	↔	^]	GS		组分隔符	45	-	61	=	77	M	93	]	109	m	125	}	
1110	E	14	♫	^N	SO		移出	30	▲	^^	RS		记录分隔符	46	.	62	>	78	N	94	^	110	n	126	~	
1111	F	15	☼	^O	SI		移入	31	▼	^-	US		单元分隔符	47	/	63	?	79	O	95	_	111	o	127	⌂	^Backspace 代码：DEL

注：表中的ASCII字符可以用“Alt + 小键盘上的数字键”方法输入。

2013/08/08

2、由题目可知其格式为`flag{ }`，所以我们可以从`flag`和`afZ_`之间的对应关系找出规律。

密文	明文	变化规律
a (97)	f (102)	+5
f (102)	l (108)	+6
Z (90)	a (97)	+7
_ (95)	g (103)	+8

可以看出其偏移量是对每个字符：从第一个字符的偏移量为5，第二个字符的偏移量为6.....第n个字符的偏移量为4+n。偏移量依次递增。

3、解密

Python版解密代码

```
ciphertext = 'afZ_r9VYfScOeO_UL^RWUc'
j = 5
for i in ciphertext:
    print(chr(ord(i) + j), end='')
    j += 1
```

java版解密代码

```java
public class Caesar {
    public static void main(String[] args) {
        String ciphertext = "afZ_r9VYfScOeO_UL^RWUc";
        char[] plaintext = new char[ciphertext.length()];
        for(int i = 0; i < ciphertext.length(); i++){ //注意i是从0开始的，所以是5+i
            plaintext[i] = (char)(((int)ciphertext.charAt(i) + 5 + i) % 128);
        }
        for (char i: plaintext) {
            System.out.print(i);
        }
    }
}
```

结果

```
flag{Caesar_variation}
Process finished with exit code 0
```

4、提交答案 `flag{Caesar_variation}`

加密密文：afZ_r9VYfScOeO_UL^RWUc
格式：flag{ }

解题链接：　　通过

flag{Caesar_variation}

解题成功