HOMEWORK 9

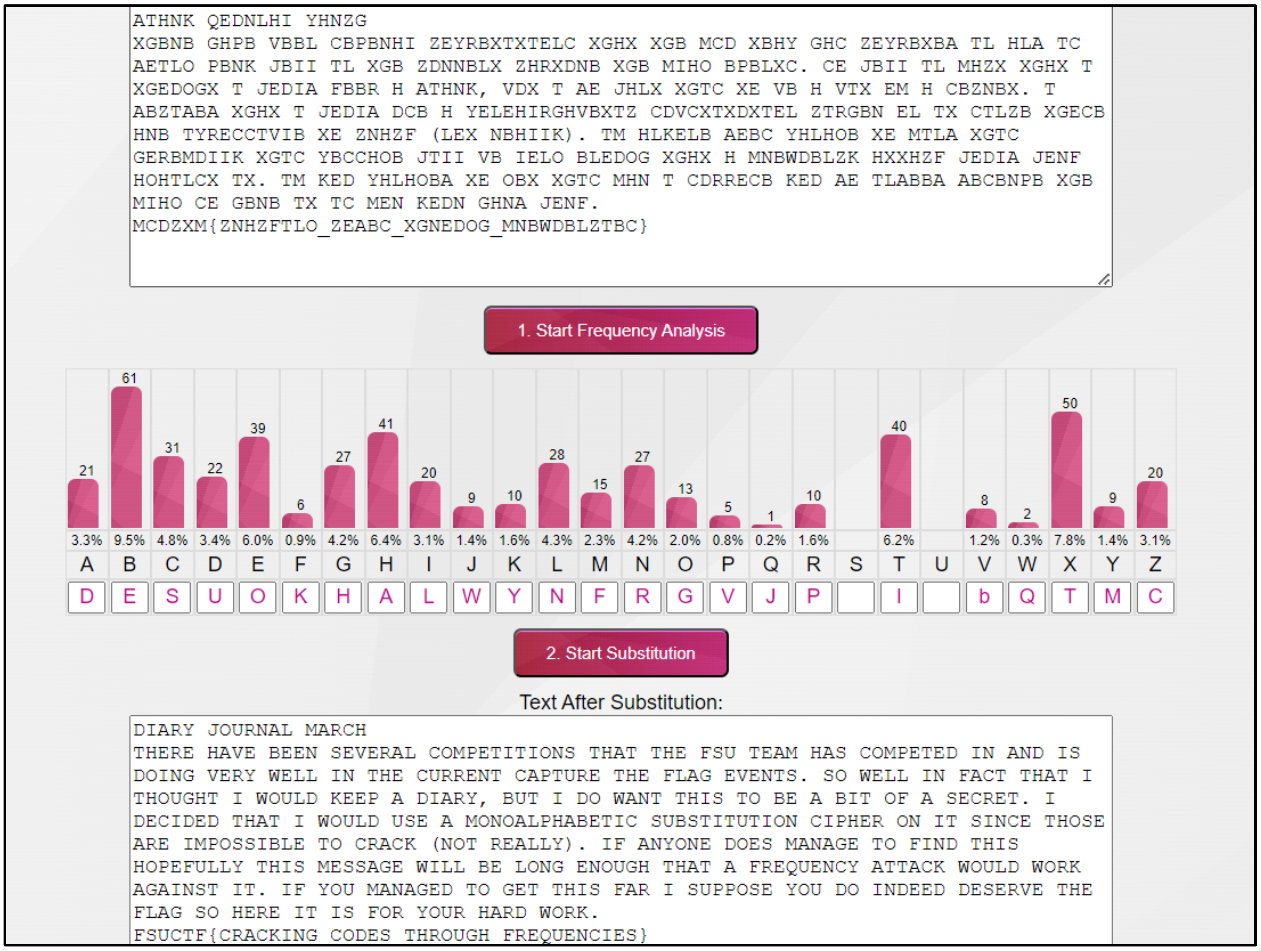
~ Purva Naresh Rumde (pr23b)

Problem ID	Captured Flag	Steps
P1	FSUCTF{CRACKING_CODES_THROUGH_FREQUENCIES}	In this problem, I put the text for frequency analysis. And after substitution I got the flag.
P2	fsuCTF{r0t4t1ng_k3y5_unL0ck_s3cr3t5}	In this problem, I simply pasted the encrypted text on cyberchef and after converting from hex and then providing the key I got the flag, since the key was “simple”.
P3	fsuCTF{rSA_M0r3_L1K3_ma7h_7hAn_cryp70}	In this problem, I put the values of c,n,e amd got the flag for each part.

1. Flag: **FSUCTF{CRACKING_CODES_THROUGH_FREQUENCIES}**

In this problem there is a text file that was provided. I then tried the frequency analysis on this text file. After the analysis I figured out the frequencies of every alphabet.

So before starting the substiituton I had fugured out that since the flag starts with FSUCTF {} so I replaced the same with the text file and that is how I replaced all the alphabets. And then I got the flag.



```
ATHNK QEDNLHI YHNZG
XGBNB GHPB VBBL CBPBNHI ZEYRBXTXTELC XGHX XGB MCD XBHY GHC ZEYRBXBA TL HLA TC
AETLO PBNK JBII TL XGB ZDNNBLX ZHRXDNB XGB MIHO BPBLXC. CE JBII TL MHZX XGHX T
XGEDOGX T JEDIA FBBR H ATHNK, VDX T AE JHLX XGTC XE VB H VTX EM H CBZNBX. T
ABZTABA XGHX T JEDIA DCB H YELEHIRGHVBXTZ CDVCXTXDXTEL ZTRGBN EL TX CTLZB XGECB
HNB TYRECCTVIB XE ZNHZF (LEX NBHIIK). TM HLKELB AEBC YHLHOB XE MTLA XGTC
GERBMDIIK XGTC YBCCHOB JTII VB IELO BLEDOG XGHX H MNBWDBLZK HXXHZF JEDIA JENF
HOHTLCX TX. TM KED YHLHOBA XE OBX XGTC MHN T CDRRECB KED AE TLABBA ABCBNPB XGB
MIHO CE GBNB TX TC MEN KEDN GHNA JENF.
MCDZXM{ZNHZFTLO_ZEABC_XGNEDOG_MNBWDBLZTBC}
```

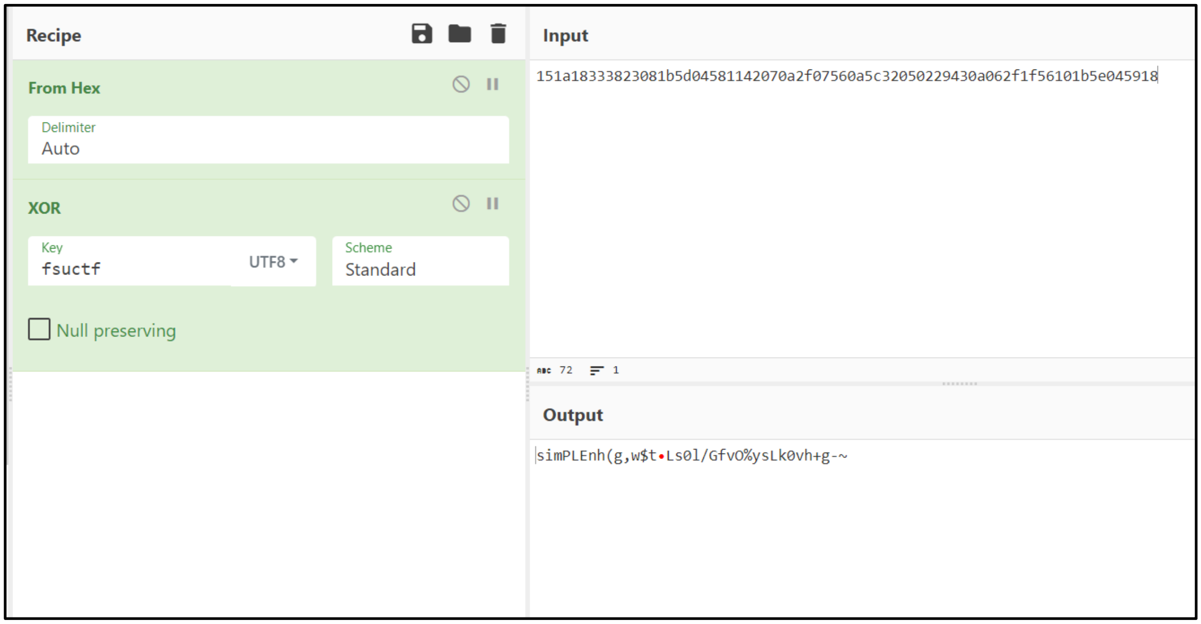
21	61	31	22	39	6	27	41	20	9	10	28	15	27	13	5	1	10		40		8	2	50	9	20
3.3%	9.5%	4.8%	3.4%	6.0%	0.9%	4.2%	6.4%	3.1%	1.4%	1.6%	4.3%	2.3%	4.2%	2.0%	0.8%	0.2%	1.6%		6.2%		1.2%	0.3%	7.8%	1.4%	3.1%
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	S	U	O	K	H	A	L	W	Y	N	F	R	G	V	J	P		I		b	Q	T	M	C

Text After Substitution:

```
DIARY JOURNAL MARCH
THERE HAVE BEEN SEVERAL COMPETITIONS THAT THE FSU TEAM HAS COMPETED IN AND IS
DOING VERY WELL IN THE CURRENT CAPTURE THE FLAG EVENTS. SO WELL IN FACT THAT I
THOUGHT I WOULD KEEP A DIARY, BUT I DO WANT THIS TO BE A BIT OF A SECRET. I
DECIDED THAT I WOULD USE A MONOALPHABETIC SUBSTITUTION CIPHER ON IT SINCE THOSE
ARE IMPOSSIBLE TO CRACK (NOT REALLY). IF ANYONE DOES MANAGE TO FIND THIS
HOPEFULLY THIS MESSAGE WILL BE LONG ENOUGH THAT A FREQUENCY ATTACK WOULD WORK
AGAINST IT. IF YOU MANAGED TO GET THIS FAR I SUPPOSE YOU DO INDEED DESERVE THE
FLAG SO HERE IT IS FOR YOUR HARD WORK.
FSUCTF{CRACKING_CODES_THROUGH_FREQUENCIES}
```

2. Flag: **fsuCTF{r0t4t1ng_k3y5_unL0ck_s3cr3t5}**

   In this problem the biggest hint was the rotating key XOR. 2 text files where provided wordlist and the encrypted cypher text. So I copied the cipher text and pasted it on CyberChef.
   After applying from hex. I tried to know the xor key and for that I just gave fsuctf as the key on the retrieved simple. So that is when I got to know that simple is the key.
   So then I gave simple as the key and that is how I got the flag.



From Hex
Delimiter: Auto

XOR
Key: fsuctf (UTF8)
Scheme: Standard
□ Null preserving

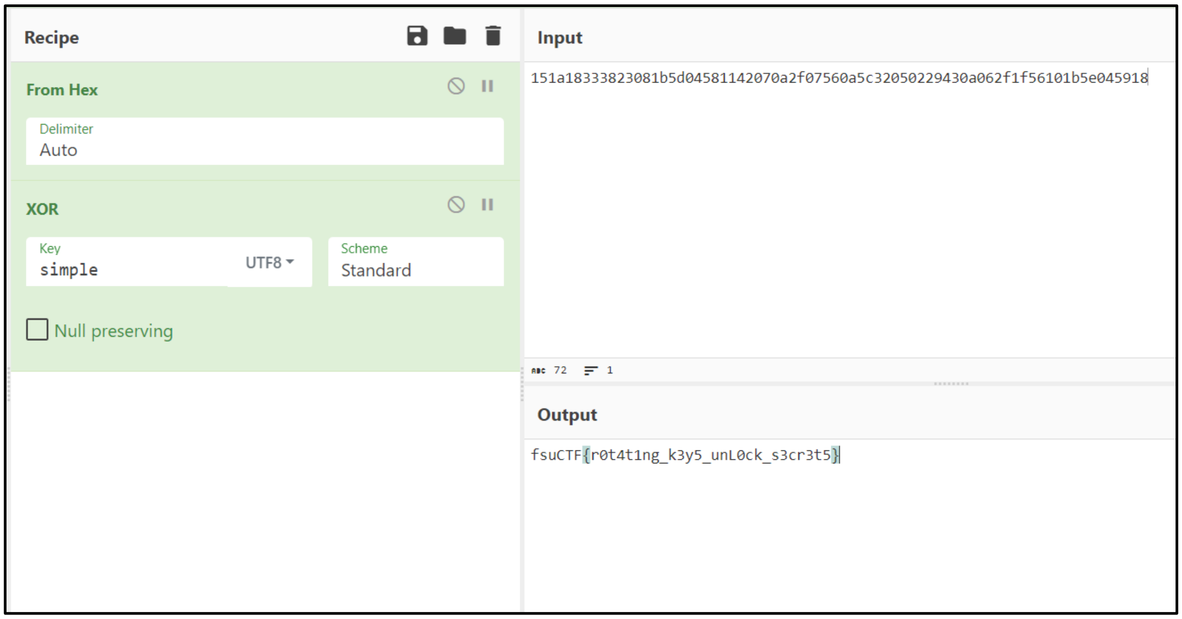
Input:

```
151a18333823081b5d04581142070a2f07560a5c32050229430a062f1f56101b5e045918
```

abc 72 ≡ 1

Output:

```
simPLEnh(g,w$t•Ls0l/GfvO%ysLk0vh+g-~
```



From Hex
Delimiter: Auto

XOR
Key: simple (UTF8)
Scheme: Standard
□ Null preserving

Input:

```
151a18333823081b5d04581142070a2f07560a5c32050229430a062f1f56101b5e045918
```

abc 72 ≡ 1

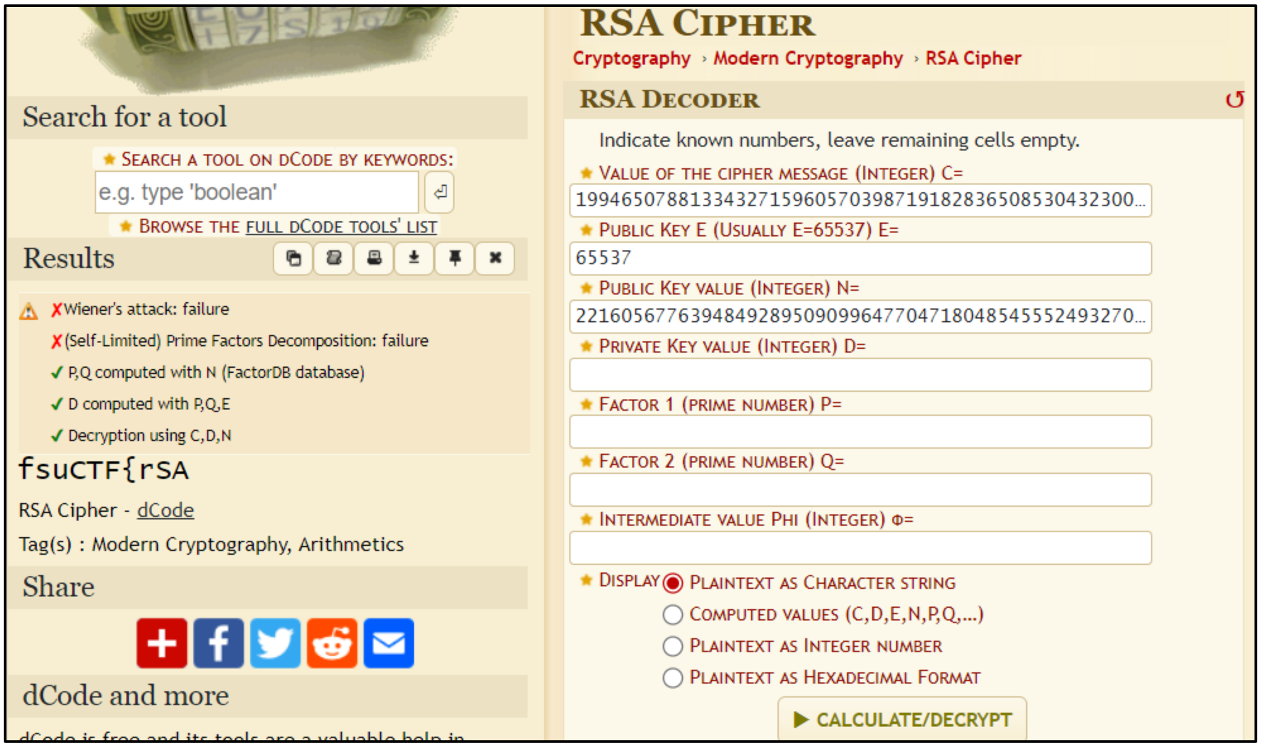
Output:

```
fsuCTF{r0t4t1ng_k3y5_unL0ck_s3cr3t5}
```

3. Flag: **fsuCTF{rSA_M0r3_L1K3_ma7h_7hAn_cryp70}**

In this problem we were provided with 2 files one python file and other a text file. The text file consisted of the values of c1, c2, c3 , e1, n1 and p. So with these values I tried the RSA cipher where I gave input of these values and got the first part of the flag.

For the second part the text file did not consist the n2, that was provided in the code part. So gathered this information from the code and that is how I generated flag from all three parts.



Search for a tool
★ Search a tool on dCode by keywords:
e.g. type 'boolean'
★ Browse the full dCode tools' list
Results

✗Wiener's attack: failure
✗(Self-Limited) Prime Factors Decomposition: failure
✓ P,Q computed with N (FactorDB database)
✓ D computed with P,Q,E
✓ Decryption using C,D,N

fsuCTF{rSA

RSA Cipher - dCode

Tag(s) : Modern Cryptography, Arithmetics

Share
dCode and more
dCode is free and its tools are a valuable help in
RSA Cipher
Cryptography › Modern Cryptography › RSA Cipher
RSA Decoder

Indicate known numbers, leave remaining cells empty.

★ Value of the cipher message (Integer) C=
1994650788133432715960570398719182836508530432300…

★ Public Key E (Usually E=65537) E=
65537

★ Public Key value (Integer) N=
2216056776394849289509099647704718048545552493270…

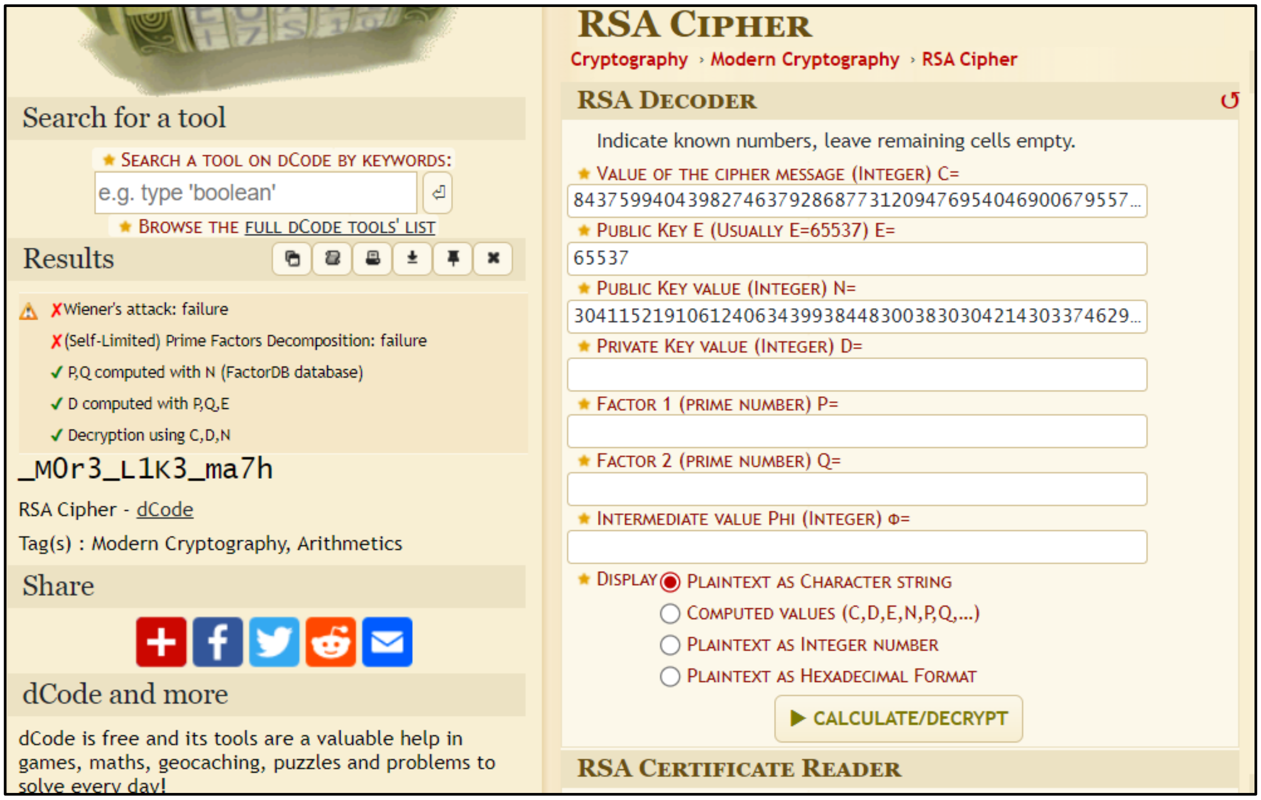
★ Private Key value (Integer) D=

★ Factor 1 (prime number) P=

★ Factor 2 (prime number) Q=

★ Intermediate value Phi (Integer) Φ=

★ Display ● Plaintext as character string
○ Computed values (C,D,E,N,P,Q,…)
○ Plaintext as Integer number
○ Plaintext as Hexadecimal Format



Search for a tool

★ SEARCH A TOOL ON DCODE BY KEYWORDS:

e.g. type 'boolean'

★ BROWSE THE FULL DCODE TOOLS' LIST

Results

⚠ ✗Wiener's attack: failure

✗(Self-Limited) Prime Factors Decomposition: failure

✓ P,Q computed with N (FactorDB database)

✓ D computed with P,Q,E

✓ Decryption using C,D,N

```
_M0r3_L1K3_ma7h
```

RSA Cipher - dCode

Tag(s) : Modern Cryptography, Arithmetics

Share

dCode and more

dCode is free and its tools are a valuable help in games, maths, geocaching, puzzles and problems to solve every day!

RSA CIPHER

Cryptography › Modern Cryptography › RSA Cipher

RSA DECODER

Indicate known numbers, leave remaining cells empty.

★ VALUE OF THE CIPHER MESSAGE (INTEGER) C=
8437599404398274637928687731209476954046900679557…

★ PUBLIC KEY E (USUALLY E=65537) E=
65537

★ PUBLIC KEY VALUE (INTEGER) N=
3041152191061240634399384483003830304214303374629…

★ PRIVATE KEY VALUE (INTEGER) D=

★ FACTOR 1 (PRIME NUMBER) P=

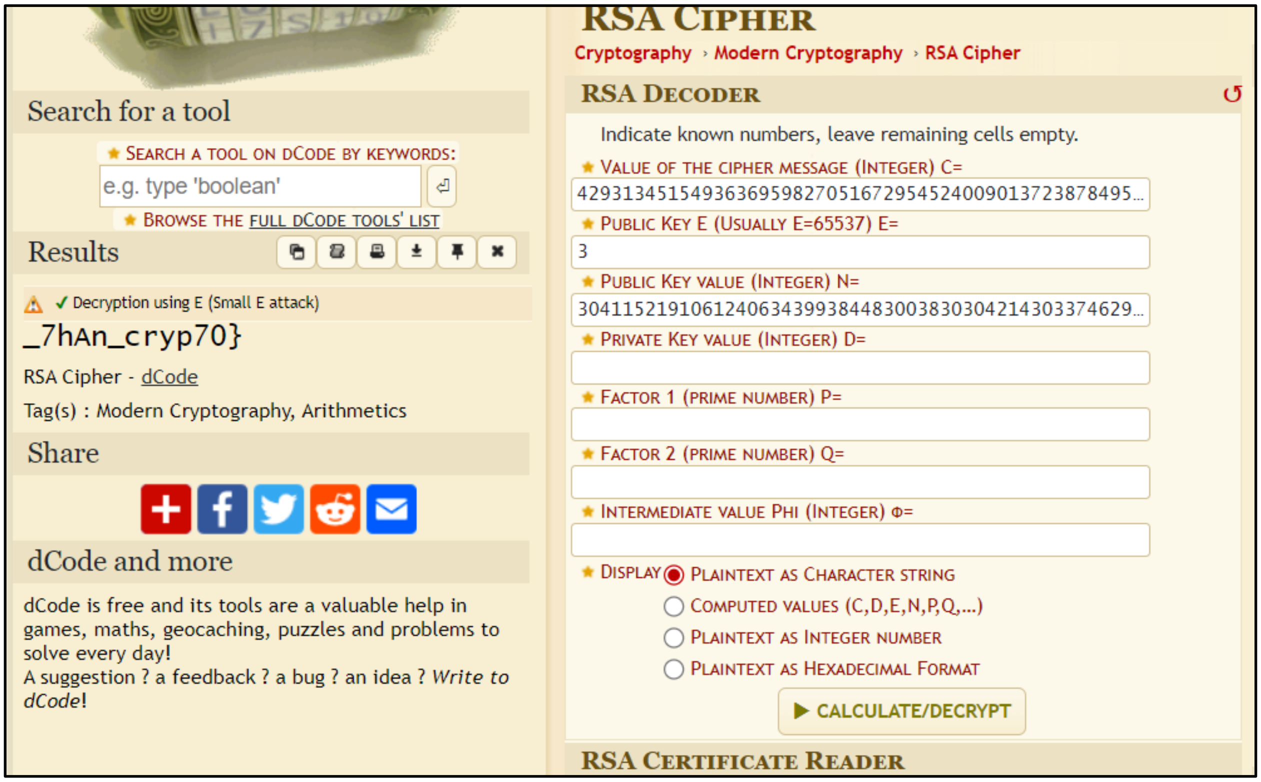
★ FACTOR 2 (PRIME NUMBER) Q=

★ INTERMEDIATE VALUE PHI (INTEGER) Φ=

★ DISPLAY ● PLAINTEXT AS CHARACTER STRING
○ COMPUTED VALUES (C,D,E,N,P,Q,...)
○ PLAINTEXT AS INTEGER NUMBER
○ PLAINTEXT AS HEXADECIMAL FORMAT

▶ CALCULATE/DECRYPT

RSA CERTIFICATE READER



Search for a tool

★ SEARCH A TOOL ON DCODE BY KEYWORDS:

e.g. type 'boolean'

★ BROWSE THE FULL DCODE TOOLS' LIST

Results

⚠ ✓ Decryption using E (Small E attack)

```
_7hAn_cryp70}
```

RSA Cipher - dCode

Tag(s) : Modern Cryptography, Arithmetics

Share

dCode and more

dCode is free and its tools are a valuable help in games, maths, geocaching, puzzles and problems to solve every day!
A suggestion ? a feedback ? a bug ? an idea ? *Write to dCode*!

RSA CIPHER

Cryptography › Modern Cryptography › RSA Cipher

RSA DECODER

Indicate known numbers, leave remaining cells empty.

★ VALUE OF THE CIPHER MESSAGE (INTEGER) C=
4293134515493636959827051672954524009013723878495…

★ PUBLIC KEY E (USUALLY E=65537) E=
3

★ PUBLIC KEY VALUE (INTEGER) N=
3041152191061240634399384483003830304214303374629…

★ PRIVATE KEY VALUE (INTEGER) D=

★ FACTOR 1 (PRIME NUMBER) P=

★ FACTOR 2 (PRIME NUMBER) Q=

★ INTERMEDIATE VALUE PHI (INTEGER) Φ=

★ DISPLAY ● PLAINTEXT AS CHARACTER STRING
○ COMPUTED VALUES (C,D,E,N,P,Q,...)
○ PLAINTEXT AS INTEGER NUMBER
○ PLAINTEXT AS HEXADECIMAL FORMAT

▶ CALCULATE/DECRYPT

RSA CERTIFICATE READER