Gloire Rubambiza
02/05/2018

ADFGVX Cipher.

1.

	A	D	F	G	V	X
A	O	R	9	E	5	X
D	P	L	K	S	Z	A
F	B	6	J	G	W	3
G	4	U	N	V	Q	T
V	0	H	M	C	8	D
X	I	F	1	2	7	Y

Clear Text: "DONT PANIC"
Matching text = VXAA GFGXDADX GFXAVG

H	E	L	P
V	X	A	A
G	F	G	X
D	A	D	X
G	F	X	A
V	G		

E	H	L	P
X	V	A	A
F	G	G	X
A	D	D	X
F	G	X	A
G	V		

Ciphered text: XFAFGVGDGVAGDX AXXA

2. A	B	E	O	R	T
A	X	G	X	D	A
X	A	D	D	G	F
D	G	A	X	G	G
A	V	A	G	G	D
V	G	A	X	G	F
D	D	D	G	X	G
A	F		G		G

B	O	A	T	E	R
X	X	A	A	G	D
A	D	X	F	D	G
G	X	D	G	A	G
V	G	A	D	A	G
G	X	V	F	A	G
D	G	D	G	D	X
F	G	A	G		

Decrypted: YOUR1STSECRETMESSAGE

03/02/2018

El Gamal Continued

Public info

p, prime

g, prim. root mod p $\quad p = 967$, $g = 37$, $b = 871$

$B = (g^b \bmod p)$

↑

Public key $\quad \Rightarrow$ Bob's "Secret key", b an integer

1. $B = 37^{871} \bmod 967 = 12$

2. Shared, partner $B = 83$, $\boxed{R = 296, \; c = 31}$ $\quad m = 464$

3. $\boxed{m = 833}$, nonce $(r) = 381$

↳ my message

4. $R = g^r \bmod p = 37^{381} \bmod 967 = 505$

$c = m \cdot B^r \bmod p = 986 \cdot 83^{381} \bmod 967 = 334$

5. shared R and C with partner

6. $c \cdot R^{p-1-b} \bmod p = 31 \cdot 296^{967-1-871} \bmod 967 = 1$

Exercises

1. Calculate $11^8 \bmod 31$

$11^4 \bmod 31 = 14\,641 \bmod 31$

$= 9$

$11^8 \bmod 31 = (11^4 * 11^4) \bmod 31$

$= (11^4 \bmod 31 * 11^4 \bmod 31) \bmod 31$

$= (9 . 9) \bmod 31$

$= 19$

2. $8^{12} \bmod 29 = 8^{8+4} \bmod 29$

$8^2 \bmod 29 = 64 \bmod 29$

$= 6$

$8^4 \bmod 29 = (8^2)^2 \bmod 29$

$= (6.6) \bmod 29$

$= 7$ *

$8^8 \bmod 29 = (8^4)^2 \bmod 29$

$= (7.7) \bmod 29$

$= 20$ *

$8^{12} \bmod 29 = 8^{8+4} \bmod 29$

$= (8^8 . 8^4) \bmod 29$

$= (20 . 7) \bmod 29$

$= \boxed{24}$