

Expectations for cryptography midterm on Thursday:

Bring a calculator and blank sheets.

Know how to encrypt/decrypt with Spartan Scytale, Playfair, ADFGVX (if I give you the table); encrypt/decrypt/cryptanalyze with $C \equiv aP + b \pmod{N}$; encode and decode digraphs; how to evaluate $\phi(n)$; add, multiply and invert in $\mathbf{Z}/n\mathbf{Z}$ and finite fields; encrypt/decrypt with a stream cipher (I would give you the algorithm for a self-synchronizing stream cipher); be able to generate a pseudo-random string if I give you p, q, g, k ; encrypt/decrypt with S-AES if I give you the order of the steps; generate a key for S-AES; know vocabulary, concepts, history and AES design. You do not need to memorize the diagrams for CBC, CFB, OFB. I will not test you on properties of mod (like Fermat's Little Theorem) specifically, though they may come up while doing a problem. There will be nothing like homework $NT - 7, 8$.

The following will be at the top of your exam:

a=0,b=1,c=2,d=3,e=4,f=5,g=6,h=7,i=8,j=9,k=10,l=11,m=12,n=13,o=14,p=15,q=16,
r=17,s=18,t=19,u=20,v=21,w=22,x=23,y=24,z=25

if $i \equiv 0 \pmod{2}$ then $W[i] = W[i - 2] \oplus \text{RCON}(i/2) \oplus \text{SubNib}(\text{RotNib}(W[i - 1]))$
if $i \not\equiv 0 \pmod{2}$ then $W[i] = W[i - 2] \oplus W[i - 1]$

nib	S-box(nib)	nib	S-box(nib)	nib	S-box(nib)	nib	S-box(nib)
0000	1001	0100	1101	1000	0110	1100	1100
0001	0100	0101	0001	1001	0010	1101	1110
0010	1010	0110	1000	1010	0000	1110	1111
0011	1011	0111	0101	1011	0011	1111	0111

Encrypt:	$b_0 \oplus b_6$	$b_1 \oplus b_4 \oplus b_7$	$b_2 \oplus b_4 \oplus b_5$	$b_3 \oplus b_5$	$\text{RCON}(1) = 10000000$
	$b_2 \oplus b_4$	$b_0 \oplus b_3 \oplus b_5$	$b_0 \oplus b_1 \oplus b_6$	$b_1 \oplus b_7$	$\text{RCON}(2) = 00110000$

a	01100001	b	01100010	c	01100011	d	01100100	e	01100101
f	01100110	g	01100111	h	01101000	i	01101001	j	01101010
k	01101011	l	01101100	m	01101101	n	01101110	o	01101111
p	01110000	q	01110001	r	01110010	s	01110011	t	01110100
u	01110101	v	01110110	w	01110111	x	01111000	y	01111001