4.1

(a) Public Modulus

$N = p \cdot q = 541 \cdot 1223 = 661643$

$(p-1)(q-1) = 540 \cdot 1222 = 659880$

Private Signing key?

$ed \equiv 1 \bmod 659880$

$159853d \equiv 1 \bmod 659880$

$d \equiv 561517$

(b) What is the signature?

$S \equiv D^d \equiv 630579^{561517} \bmod 661643$

$S \equiv 206484$

4.2

Using $S^e \bmod N$

1) S

$876453^{87953} \bmod 1562501$

↳ $772481 \neq 119812$

2) S'

$870099^{87953} \bmod 1562501$

↳ $161153 \equiv 161153$

3) S''

$602754^{87953} \bmod 1562501$

↳ $586036 \equiv 586036$

Signatures S' AND S'' ARE BOTH VALID SIGNATURES

4.5 Elgamal Signature $p = 6961$, $g = 437$

(a) $a = 6104$ Find Public verification key

$$A \equiv g^a \bmod p$$

$$\equiv 437^{6104} \bmod 6961$$

$A \equiv 2065$

(b) What is the signature?

$D = 5584$, $k = 4451$

$$S_1 \equiv g^k \bmod p \qquad S_2 \equiv (D - aS_1)k^{-1} \bmod (p-1)$$

$$\equiv 437^{4451} \bmod 6961$$

$S_1 \equiv 3534$ $\rightarrow S_2 \equiv (5584 - 6104 \cdot 3534)(491)$

$S_2 \equiv 5888$

$(S_1, S_2) = (3534, 5888)$

4.6

$A^{S_1} S_1^{S_2} \bmod p$ Should equal $g^D \bmod p$

1) $4250^{4129} \cdot 4129^{5575} \bmod 6961 \equiv 231$

$437^{1521} \bmod 6961 \equiv 231$

2) $4250^{3145} \cdot 3145^{1871} \bmod 6961 \equiv 6208$

$437^{1837} \bmod 6961 = 2081$

3) $4250^{2709} \cdot 2709^{2944} \bmod 6961 = 2243$

$437^{1614} \bmod 6961 = 2243$

VALID SIGNATURES: $(S_1, S_2) = (4129, 5575)$

$(S_1, S_2) = (2709, 2944)$

4.9 DSA Public Parameters $(p, q, g) = (22531, 751, 4488)$
secret signing key $a = 674$

(a)
$$A = g^a \equiv 4488^{674} \bmod 22531$$
$$A \equiv 4940 \bmod 22531$$

(b) Find Signature - $D = 244$, $k = 574$

$$S_1 \equiv (g^k \bmod p) \bmod q \qquad S_2 \equiv (D + aS_1)k^{-1} \pmod q$$

$$S_1 \equiv (4488^{574} \bmod 22531) \bmod 751 \qquad S_1 \equiv 444$$

$$S_2 \equiv (244 + 674 \cdot 444)\, 574^{-1} \bmod 751 \qquad S_2 \equiv 688$$
$$\equiv 637 \cdot 297 \bmod 751$$
$$(S_1, S_2) = (444, 688)$$

4.10 DSA Public Parameters $(p, q, g) = (22531, 751, 4488)$
$A = 22476$

(a) Is $(S_1, S_2) = (183, 260)$ valid for $D = 329$?

$$V_1 \equiv DS_2^{-1} \bmod q \qquad V_2 \equiv S_1 S_2^{-1} \bmod q$$
$$\equiv (329)\, 260^{-1} \bmod 751 \qquad \equiv (183)\, 260^{-1} \bmod 751$$
$$\equiv 329 \cdot 26 \qquad 183 \cdot 26 \bmod 751$$
$$\equiv 293 \bmod 751 \qquad \equiv 252 \bmod 751$$

$$(g^{V_1} A^{V_2} \bmod p) \bmod q = S_1 ?$$
$$\equiv (4488^{293}\ 22476^{252} \bmod 22531) \bmod 751$$
$$\equiv 6191 \bmod 751$$
$$\equiv 183 \bmod 751 \quad \checkmark \text{ Equal to } S_1$$
Signature is Valid

(b) $(s_1, s_2) = (211, 97)$, $D = 432$

$V_1 \equiv D s_2^{-1} \bmod q$

$\equiv 432 \cdot 97^{-1} \bmod 751$

$\equiv 432 \cdot 511 \bmod 751$

$\equiv 709 \bmod 751$

$V_2 \equiv s_1 s_2^{-1} \bmod q$

$\equiv 211 \cdot 97^{-1} \bmod 751$

$\equiv 211 \cdot 511 \bmod 751$

$\equiv 428 \bmod 751$

$(g^{V_1} A^{V_2} \bmod p) \bmod q = s_1 ?$

$\hookrightarrow (4488^{709} \cdot 22476^{428} \bmod 22531) \bmod 751$

$s_1 \neq 224$ Signature NOT VALID

5.3 (a) Permutations of the set $\{A, B, C\}$

$\{A,B,C\}, \{A,C,B\}, \{B,A,C\}, \{C,A,B\}, \{B,C,A\}, \{C,B,A\}$

3 elements $\rightarrow 3! = 3 \cdot 2 \cdot 1 =$ 6 Permutations

(d)

$7! = 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1 =$ 5040 ways

5.4 (c) Nine symbols A, A, A, A, B, B, B, C, C

how many different nine letter words can be formed

$$\text{Words} = \frac{9!}{4! \cdot 3! \cdot 2!} = 1260 \text{ words}$$

9. (a) $P(n,r) = \frac{n!}{(n-r)!}$

$$P(25,3) = \frac{25!}{22!} = \frac{25 \cdot 24 \cdot 23 \cdot \cancel{22!}}{\cancel{22!}} = 13800 \text{ possible outcomes}$$

(b) $C(n,r) = \frac{n!}{r!(n-r)!} = \frac{25!}{3!(22!)} = \frac{25 \cdot 24 \cdot 23 \cdot \cancel{22!}}{3 \cdot 2 \cdot 1 \cdot \cancel{22!}} =$ 2300 possible outcomes

10. "to be or not to be" using "hamlet"

↓

7 0 12 11 4 19

p:	t	o	b	e	o	r	n	o	t	t	o	b	e
+k:	7	0	12	11	4	19	7	0	12	11	4	19	7
C:	a	o	n	p	s	k	u	o	f	e	s	u	l

19+17 mod 26

ciphertext: aonpskuofesul

11. "pzazx zpctb iypq", using "nickel" → 13 8 2 10 4 11

C:	p	z	a	z	x	z	p	c	t	b	i	y	p	q
-k:	13	8	2	10	4	11	13	8	2	10	4	11	13	8
p:	C	R	Y	P	T	O	C	U	R	R	E	N	C	Y

plaintext: Crypto currency