Name:

Information Assurance: Homework 2 - Comments

Grade each question to 25 points.

Due September 8, 2010 on compass.

1. Policy or mechanism. For each item below, is it a policy or an enforcing mechanism? If it is a policy, identify a mechanism that could enforce it. If it is a mechanism, identify a policy it could be enforcing.

5 points each.

a) Data classified as critical must be strongly encrypted when moving over public networks.

I'd argue for this being being a mechanism. It would be implementing a policy like, the confidentiality of classified data must be adequately protected when moving over the network.

However you do see statements like this in corporate policies (I think it is in the Uillinois Policy). So I'd give all or most points if they argue it as a policy. In that case, the mechanism would be specification of the specific algorithm or tool, e.g. Data classified as critical, must be classified by AES with at least a 192 bit key when traversing a public network.

b) All desktop computers must have password-based screen savers configured to go on after 30 seconds.

Definitely a mechanism. Could be implementing the policy, only authenticated and verified individuals may access information on corporate computers.

c) Students and staff may not loan their their university key cards to other individuals.

Mechanism. Enforcing a policy of only appropriately cleared students and staff may enter Siebel after hours.

Many people argued this as a policy. They gave the matching mechanism as checking the photo on the ID at appropriate places. I think it argues better as a mechanism, because the keycard is a mechanism. The keycard in and of itself doesn't have any value, but the keycard acts as an authentication mechanism that enables you to enforce policies that need to restrict physical access.

d) Only residents of Urbana may enroll their children in Urbana schools.

Policy. An enforcing mechanism could be the procedure of having the parents show a deed or a lease to housing within the school district.

e) Meijer's cashiers must check the ID of anyone who appears to be under 40 when they purchase alcohol.

Name:

Mechanism. Enforcing the policy of Meijer's employees may not break Illinois law by selling alcohol to minors.

2. You own a jewelry store. In your neighborhood, there is a 15% chance of a store like yours being the victim of a robbery during the course of the year. On average, your store has $100,000 in cash and products on hand. You are considering two controls. The first option is to hire a full time guard at the cost of $5,000 per month. Based on experience in your industry, this should reduce your risk of robbery to 3% over a year. The second option is to hire an alarm/monitoring company. They will install cameras and have a staff at their offices reviewing the camera feeds. This will reduce the risk of a non-recoverable robbery to %8 and will cost $2,000 a month.

6 points for each section.

a) What is your current annual loss expectancy (ALE) (you've implemented neither control)?

Answer: 100000 x 0.15 = 15000

For parts b and c, a number of people used the cost of a month instead of the cost of a year in calculating the risk leverage. Since the top of the calculation is the risk impact over a year, the bottom of the calculation should also be with respect to a year. If you adjusted the risk impact change to also be a month, that would also be ok.

b) Compute the risk leverage for the first option (hiring a guard).

Answer:

Risk exposure

before control = 100000 x 0.15 = 15000

Risk exposure

after control = 100000 x 0.03 = 3000

Risk Leverage = ((risk exp. before control) – (risk exp. after))/

(cost of control)

= (15000 – 3000)/(5000 x 12)

= 0.2

Name:

c) Compute the risk leverage for the second option (install cameras and employ the monitoring company).

Answer:

Risk exposure

before control = 100000 x 0.15 = 15000

Risk exposure

after control = 100000 x 0.08 = 8000

Risk Leverage = ((risk exp. before control) – (risk exp. after))/

(cost of control)

= (15000 – 8000)/(2000 x 12)

= 0.2917

d) Based on the risk leverage computation, which option should you go with?

Not a very clear winner in this case. I'd go with the second option, since it has a slightly higher risk leverage. Some people may argue that neither option is any good because the cost in a year is higher than the expected savings. I'd give partial credit for that logic.

3. Consider the rail cipher or the n-columnar transposition cipher:

6 points each section.

a) Encrypt the following phrase using the rail cipher or 2-columnar transposition cipher: **Now is the time for all good men to come to the aid of their country.**

Ans: Nwshtmfrlgomnooeohadfhicutyoiteieoalodetcmtteioteronr.

No

wi

st

he

ti

me

fo

ra

Name:

ll

go

od

me

nt

oc

om

et

ot

he

ai

do

ft

he

ir

co

un

tr

y.

b) Decrypt the following phrase using a 3-columnar transposition

TQCRNXMDEHADHUKOFJPOREZOEIBWOUEVTLYG

Answer: The quick brown fox jumped over the lazy dog

TQCRNXMDEHAD

HUKOFJPOREZO

EIBWOUEVTLYG

c) Given a piece of cipher text, how would you first test to see if it was a transposition cipher?

Answer:

If 1-gram frequencies match English

frequencies, but other n-gram frequencies do

not, probably transposition

Name:

d) Assuming it appears to be a transposition cipher, and you think it is probably a n-columar cipher, how would you start determining the **n** for the n-columnar transposition?

Answer: Rearrange letters to form n-grams with highest

frequencies

4. Consider Vigenere cipher:

6 points each section.

a) Use the Vigenere tableau at the end to encrypt the phrase "Labor Day" with the key "work".

Answer:

P Text : L A B O R D A Y

Key: W O R K W O R K

C Text : H O S Y N R R I

b) Use the Vigenere tableau to decrypt "YHPRWELEUUXAPIY" with the key "fall".

Answer:

C Text: YHPR WELE UUXA PIY

Key : FALL FALL FALL FAL

P Text: THE GREAT PUMPKIN

c) Determine the key and decode the Vigenere encrypted text posted at http://www.cs.illinois.edu/class/fa10/cs461/assignments/cipher.txt. You may use automated tools such as the applet discussed in class http://math.ucsd.edu/~crypto/java/EARLYCIPHERS/Vigenere.html.

Answer:

ETTU

FRIENDS ROMANS COUNTRYMEN LEND ME YOUR EARS I COME TO BURY CAESAR NOT TO PRAISE HIM

Name:

THE EVIL THAT MEN DO LIVES AFTER THEM
THE GOOD IS OFT INTERRED WITH THEIR BONES
SO LET IT BE WITH CAESAR THE NOBLE BRUTUS
HATH TOLD YOU CAESAR WAS AMBITIOUS
IF IT WERE SO IT WAS A GRIEVOUS FAULT
AND GRIEVOUSLY HATH CAESAR ANSWERD IT
HERE UNDER LEAVE OF BRUTUS AND THE REST
FOR BRUTUS IS AN HONOURABLE MAN
SO ARE THEY ALL ALL HONOURA BLEME NCOME ITOSP EAKIN CAESA
RSFUN ERALH EWASM YFRIE NDFAI THFUL ANDJU STTOM
EBUTB RUTUS SAYSH EWASA MBITI OUSAN DBRUT USISA
NHONO URABL EMANH EHATH BROUG HTMAN YCAPT IVESH
OMETO ROMEW HOSER ANSOM SDIDT HEGEN ERALC OFFER
SFILL DIDTH ISINC AESAR SEEMA MBITI OUSWH ENTHA
TTHEP OORHA VECRI EDCAE SARHA THWEP TAMBI TIONS
HOULD BEMAD EOFST ERNER STUFF YETBR UTUSS AYSHE
WASAM BITIO USAND BRUTU SISAN HONOU RABLE MANYO
UALLD IDSEE THATO NTHEL UPERC ALITH RICEP RESEN
TEDHI MAKIN GLYCR OWNWH ICHHE DIDTH RICER EFUSE
WASTH ISAMB ITION YETBR UTUSS AYSHE WASAM BITIO
USAND SUREH EISAN HONOU RABLE MANIS PEAKN OTTOD
ISPRO VEWHA TBRUT USSPO KEBUT HEREI AMTOS PEAKW
HATID OKNOW YOUAL LDIDL OVEHI MONCE NOTWI THOUT
CAUSE WHATC AUSEW ITHHO LDSYO UTHEN TOMOU RNFOR
HIMOJ UDGME NTTHO UARTF LEDTO BRUTI SHBEA STSAN
DMENH AVELO STTHE IRREA SONBE ARWIT HMEMY HEART
ISINT HECOF FINTH EREWI THCAE SARAN DIMUS TPAUS
ETILL ITCOM EBACK TOME

d) Describe how you determined the period. Make sure you do more than just mess about with the applet.

Name:

The student should either discuss looking for repetitions or computing the IC or both. The should not get full points for just playing around with the applet.

Some folks described playing around with the applet very systematically to find the period. I have no doubt that you could do that. However, since the question very specifically was asking for approaches that did not involve the applet, you did not get full points for such answers.

Name:

	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
A	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
B	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	a
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
F	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
H	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
I	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
J	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
K	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
L	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
Q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
R	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
S	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
T	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
U	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
V	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
W	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
X	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
Y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
Z	z	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