

Information Assurance: Midterm 1 – Answer Key

Multiple Choice – 2 points each

- Which of the following most accurately defines **vulnerability**.
 - A set of circumstances that has the potential to cause loss or harm.
 - Techniques for keeping data and resources hidden.
 - A weakness in the system that can be exploited to cause harm.*
 - Techniques for detecting unexpected behavior.
- What is the name for the following equation?
$$\frac{((\text{Risk Exposure}) - (\text{Risk Exposure after Control}))}{(\text{Cost of control})}$$
 - Risk Leverage*
 - Control costs benefits analysis
 - Annualized Loss Exposure
 - Risk Impact
- What type of cipher is AES?
 - Substitution
 - Transposition
 - Product*
 - Feistel Network
- Which of the following is **not** a standard AES key length?
 - 128
 - 160*
 - 192
 - 256
- Which of the following uses ciphertext to generate the keystream?
 - AES Electronic Codebook (ECB)
 - DES Cipher Feedback (CFB) mode*
 - AES Output Feedback (OFB) mode
 - AES Cipher Block Chaining (CBC) mode
- The cryptographic strength of RSA depends on which hard problem?
 - Discrete logarithms
 - Factoring large primes*
 - Bin packing
 - Elliptic curves

7. Which element is key to the non-linearity in the DES algorithm?
 - a. Key schedule
 - b. Splitting and swapping left and right halves of the data
 - c. Initial permutation
 - d. *Substitution boxes*

8. Which best identifies the purpose of an organizational security policy?
 - a. *A means of defining the secure states of the system*
 - b. Blueprint for the security implementation
 - c. Document to satisfy legislative requirements
 - d. A means of tracking the latest in security technology

9. Consider a double encryption of the form $C = E_{k_1}(E_{k_2}(P))$, where k_1 and k_2 are n bits long. What attack shows that the number of keys that must be checked to break a ciphertext/plaintext pair is 2^{n+1} instead of 2^{2n} .
 - a. Man-in-the-middle attack
 - b. Avalanche attack
 - c. Birthday attack
 - d. *Meet-in-the-middle attack*

Short answer

10. (5 points) If you and a colleague had to use a cipher by hand in the field, which one of the following ciphers would you select and why?
- Caesar
 - Vigenere
 - n-Transposition
 - Book cipher
 - One time pad

It was hard to take points off on this one, because most people provided some reasonable justification for their choice.

Choices a through d can be attacked through language statistics, so none of these are really secure today. Caesar cipher is very breakable with only 26 keys so I would choose one of the other options that are also still pretty easy to do by hand, but perhaps provide a bit more of a challenge to a casual observer.

There could be reasonable justifications for Vigenere and n-Transposition. I would choose the Book Cipher. From a key distribution perspective, sharing information about key texts through an alternate channel would be much easier than distributing the more secure one-time pad. Unlike Vigenere, discovering the period in the ciphertext would be quite difficult.

The main weaknesses of the book cipher are the single point of failure. If your opponent discovers your source of keys, you are lost. The keys are by definition widely available. Also, the resulting text is a combination of natural language and so still carries some of the language statistical characteristics, unlike one time pad.

Of course most all of these are better choices than using Pig Latin as someone did while organizing gang reprisals.

http://www.schneier.com/blog/archives/2007/08/code_talking_fo.html

11. (12 points) For each of the following hashing functions state why that function would make a good cryptographic hash, or state why it would not.

For parts b,c, and d, many people got the overall answer right, but their reasoning was weak. I was looking for a common on block size and strength with respect to a brute force attack. Many people mentioned the self healing aspects of CBC. However, this is only an issue for decryption and so doesn't affect the crypto hash one way or another.

a. (2 points) 256 cyclic redundancy check (CRC)

Not good. It uses a linear combination of bits, so it is computationally easy to adjust a file to match a particular CRC.

b. (2 points) 64 bit DES Cipher Block Chaining (CBC) MAC

Not good. The hash size is too small. If the opponent has the key, he could use brute force to find a message variation with the same hash.

c. (2 points) SHA-256

Good. Even with the new attacks on SHA, the 256 bit version is still beyond brute force attacks.

d. (2 points) 256 AES-CBC MAC

Good. Larger size protects it from brute force attack. Algorithm has good one way properties.

e. (4 points) You need to post crypto hashes of your company's binaries on a central web site. Your customers fetch the binaries from a variety of mirrored sites and they need a way to ensure that the downloaded binary is indeed the legitimate copy. Which of the hash functions listed in this question would you use? Why?

I'd use the SHA-256. We want a keyless hash, so everyone can independently verify the posted hash. SHA-256 has good one way properties and is large enough to avoid brute force attack.

12. (9 points) You have been hired by a company to review the communication confidentiality design created in house. Obviously the designers had not taken CS461. Identify the three worst security design errors and describe the problems caused by each of these three errors.

In the SecureComm architecture, we avoid the overheads of installing a PKI infrastructure by relying on a simpler approach of manually distributed shared keys between all pairs of communicators. Since the organization only has 25 communicators which will eventually grow to 50 over the next five years or so, we feel this approach will cost less in software and time than dealing with a full PKI solution. The keys will be passed to communicators via a separate channel such as a floppy disk or thumb drive, so the sensitive key will not be sent in the clear.

The master key file includes all the pairwise shared keys, and it can be stored on the central server. It will be stored under a very restrictive access control, so only members of the Administrative group can access the file to add or distribute keys. The master key file also provides a natural key escrow benefit. If an employee loses his or her key or leaves the organization, the administrator can access the appropriate keys from the master key file to access his or her networked conversations.

The shared key will be used in a block encryption algorithm designed by us called SuperCrypt. The algorithm is more sophisticated than AES, plus it has the benefit that it is proprietary so the attacker will not be able to attack the structure of the encryption algorithm. The SuperCrypt algorithm will be run in Electronic Code Book mode. The message integrity will be tracked by a HMAC-SHA crypto hash in the message.

There were embarrassingly many problems to choose from here.

Error 1: Manually distributing shared keys are going to cause many problems. Keys will not be updated frequently enough because of the hassle factor. The physical media used to distribute keys will be lost or stolen. As new users are added the number of keys will grow as a square (n^2). Even for $n=25$ or 50 , this is a lot of deal with.

Error 2: Long lived keys are used for bulk encryption making the problems of error 1 worse. There will be many opportunities for the attacker to gather information about the ciphertext. Once the pair key is broken, the attacker has access to all future communication until the long lived key pair is updated.

Error 3: Using a new proprietary encryption algorithm. The algorithm has not been reviewed. Even experts in cryptography have errors in their algorithms. The attacker will undoubtedly eventually find the algorithm and then can leverage those weaknesses.

Error 4: The “key escrow” of a single master file does not meet escrow requirements. There is no audit of key access. There is complete disclosure once the key between a pair of communicants is provided.

Error 5: The encryption algorithm is run in ECB. This means that identical plaintext blocks will have the same ciphertext. This is made worse by the long lived keys.

Error 6: One might be concerned by the use of HMAC-SHA. The 160 bit SHA hash has new attacks that make it vulnerable to brute force attacks. Though given the other issues in this design, this is probably one of the lower concerns.

Error 7: Key storage. If the keys are only protected by the OS access control, once the attacker can gain root access (or sufficiently privileged access) to the server, he has all the keys.

13. (14 points total) Alice is setting up a RSA key pair. She has selected $p=13$ and $q=11$
- What is n ? (1 point)

$$n = p * q = 143$$

- What is $\Phi(n)$? (1 point)

$$\Phi(n) = (p-1) * (q-1) = 120$$

- She has picked $e=13$. Which of the following would work for d : 11, 37, 119? Why?(2 points)
- $$e * d \text{ mod } \Phi(n) = 1$$
- $$13 * 37 \text{ mod } 120 = 1$$

- What values can be posted publicly and still preserve the security of the key pair?(2 points)

n, e

Many people added p and q . However, this is the factorization of n . With that information, an attacker can break a key pair.

- What RSA operation would Alice apply to a message m to convince Bob that she originated m ?(1 point)

Signing, that is encrypting with Alice's private key

$$C = m^d \text{ mod } n$$

- Apply that operation to the message EXAM. Assume a block size of one character and a character encoding of letters to numbers starting with A=1. (3 points)

$$EXAM = 5 \ 24 \ 1 \ 13$$

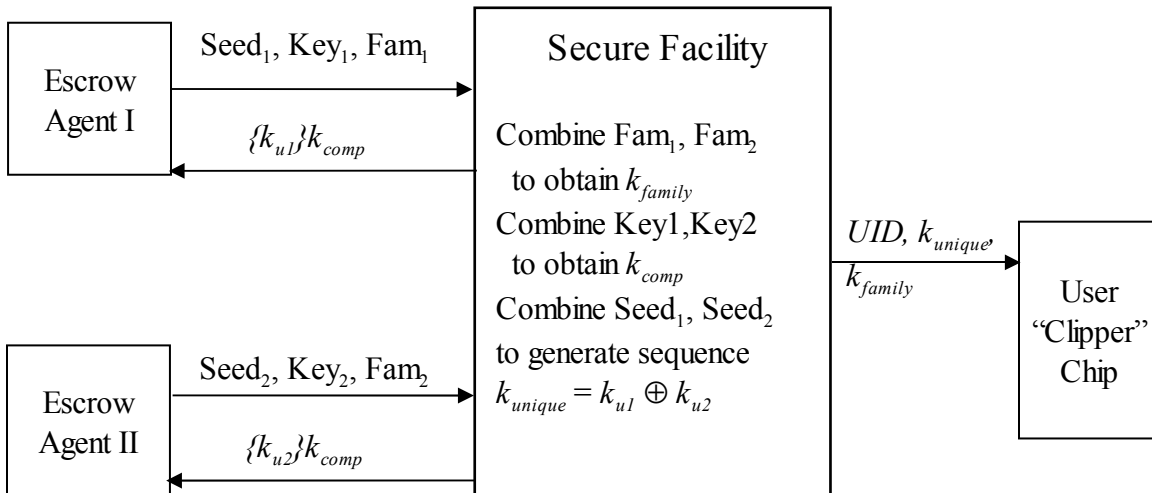
$$5^{13} \text{ mod } 143 = 135, 24^{13} \text{ mod } 143 = 128, 1^{13} \text{ mod } 143 = 1, 13^{13} \text{ mod } 143 = 117$$

- Alice has picked a session key k . Assume Alice already has access to Bob's public key. How should Alice compose a message to Bob to pass the session key while preserving confidentiality and integrity of data and identity. (4 points)

She should first sign the key with her private key to prove that she originated the message. Then she should encrypt with Bob's public key for confidentiality.

$$(k \text{ session}^{13} \text{ mod } 143)^{k \text{ BobPub}} \text{ mod } n \text{ Bob}$$

14. (15 points) You are hired to perform a risk analysis for an organization that is considering deploying a key escrow system similar to the Escrow Encryption Standard (or Clipper Chip system) discussed in class. Outline of the major components is shown below.



a. Name two risks they may be trying to control by deploying such a system. (3 points)

Employee losing key and thus data.

Being able to respond to court orders.

Concern about employee not acting in the best interest of the company.

Many people answered this part with risks to the escrow system itself.

b. Would you choose to perform a qualitative or a quantitative risk analysis? Why? (2 points)

Qualitative. It is very difficult today to assign real, reasonable numbers to value of digital assets and probability of a risk occurring. While computing real hard numbers is in some sense more satisfying and may make more sense to the business folks, the validity of the numbers is questionable unless you have good faith in your base valuations and risk probabilities. Computing a relative ordering of value and risk is much faster and often good enough to ensure that we address the most important risks first.

c. What are two assets in the key escrow system? (3 points)

The kunique, unique keys for each clipper chip.

The audit trails.

The physical clipper chips

- d. What are two vulnerabilities in the key escrow system? (3 points)

*Escrow agents could collude to gain access to the kunique without proper authorization
The user could try to prevent the LEAF information from his clipper chip from being escrowed.*

The secure facility could be bugged and the kunique could be stored away as they are generated or retrieved

Once a kunique is retrieved with authorization it could be used to access information bound the scope of the original retrieval authorization.

- e. Identify two threat sources and a motivation for each threat source. (4 points)

Competitor: Gain access to sensitive communication for corporate espionage or destroy the escrow values to prevent later recover (destroy data).

Insider: Gain access to others sensitive communication to gather interesting information for personal promotion for for sale.

Cleaning staff: Depending on sophistication may just steal chips for resale. Or may try to steal kunique for resale to competitors.

15. (8 points total, 2 points each) Is the following part of a policy or part of a mechanism
a. File system access control list

Mechanism

- b. Departmental procedure for entering student information

Mechanism

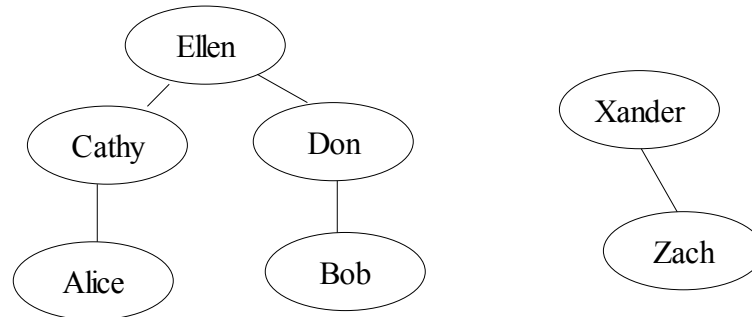
- c. Department must prevent confidential information from being revealed to the public.

Policy

- d. Confidential information must be protected, and confidential information includes employee home address.

Policy

16. (12 points) Consider the certificate authority hierarchy below. In this question the notation *signer*<<*signee*>> means that *signer* has signed the certificate of *signee*.



There was confusion for some on the basic idea of a verifying a chain of certificates in the certificate hierarchy. There was also confusion on some terminology

- *Public key* – The public portion of a key pair. Stored inside a certificate.
- *Signature* – Result of an encryption using an entity's private key generally over a hash of a document.
- *Certificate* – A binding of public key information and an entity's identity. Validity of the certificate is generally proved through signatures.

- a. (4 points) Alice receives Bob's certificate, Don<<Bob>>. What information does Alice need to verify this certificate?

Presumably Alice has Ellen's certificate, since Ellen is the root of her organization's hierarchy. Thus, if Alice had Don's certificate (Ellen<<Don>>), she could use Ellen's certificate to verify Don's, and Don's certificate to verify Bob's.

- b. (4 points) If Alice is concerned about a man-in-the middle attack, what is the minimal information should she fetch from a separate, secure channel to store on her computer?

She needs retrieve the root certificate (<<Ellen>>) from a separate, secure channel. Otherwise, Eve could intercept the request for Ellen's certificate and substitute her own. No one vouches for Ellen, so there would be no way to detect the substitution.

- c. (4 points) Alice receives Zach's certificate, Xander<<Zach>>. Zach is from a different organization. What additional information does Alice need to verify Zach's certificate? Can she meaningfully verify Zach's certificate? What change in the certificate authority relationships would help?

She needs the root certificate of the other organization's hierarchy, <<Xander>>. However, there is no reason she should put faith in the other organizations hierarchy. If the Xander and Ellen certificates were cross signed Xander<<Ellen>> and Ellen<<Xander>>, Alice could leverage her trust in Ellen to verify the authenticity of the other organization's root.

17. (4 points) Consider a Vigenere encryption $C = E(k, \text{msg})$.
- Assuming you are given a ciphertext and the length of the key, what is an upper bound on the number of keys you must test before you are guaranteed to break the key?

Assume p is the period or the length of the key and n is the size of the alphabet. The number of keys to search is n^p

- Consider double encryption where the two Vigenere keys are of the same length, i.e., $C = E(k_1, E(k_2, \text{msg}))$ where $\text{length}(k_1) = \text{length}(k_2)$. What is an upper bound on the number of cases you must test before you are guaranteed to break the key?

Since the key lengths are the same, the two substitution maps can be composed into a single map. Thus the two keys can be composed into a third key. So the number of keys to search is the same as in part a, n^p

18. (3 points) Use the attached Vigenere's tableau to decrypt the following message encrypted with the Vigenere's key of EGB (461).

XNFITE

THEEND

A number of people encrypted the message again, instead of decrypting it.

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