Submitted Sep 6 at 9:54am

Question 1 — 6 / 6 pts

Read the dramatic story below and pair the following *terms* with the underlined words in the text. Each term should be mapped only once.

Terms (listed alphabetically): *asset, assumption, attack, attackers, countermeasure, harm, month, physical control, security property, threat, value, vulnerability.*
Example: month = May

Story: For its storage needs, company BESTONE uses cloud services offered by storage provider, which recently publicly reported that in the past data leakage may have happened after a server breach by known activist hackers BESTHAC. A product engineering team at BESTONE is working on a number of sensitive documents—namely, 15 patent applications related to a new product release scheduled for May 2017. Due to the above report, and to protect the confidentiality of their proprietary data, the team manager Alice Ace requests that all such files are protected using strong encryption. The team's security expert Bob Best purchases a special appliance device called BESTPAD which, according to the vendor's web site, provides one-time encryption using (A) rekeying (namely, the encryption key is used 5 times before being renewed) and (B) hardware-based protection (namely, the encryption key cannot be leaked from the appliance as long as it operates in "air-gap" mode, i.e., stored in a locked room disconnected from any network). Bob Best justifies his choice above as "the most efficient solution for protecting against hackers with a lack of cryptanalysis expertises." In the second day of a business expo in March 2017, competitor company BESTERONE releases a product that supports most of the functionality of the product for which Alice Ace had just given an early feature presentation. The day ends with an estimated $1B damage for BESTONE and Alice Ace and Bob Best looking for new jobs.

Correct!	asset	proprietary data
Correct!	assumption	lack of cryptanalysis exp
Correct!	attack	server breach
Correct!	attackers	hackers
Correct!	countermeasure	encryption
Correct!	harm	$1B damage
Correct!	physical control	"air-gap"
Correct!	security property	confidentiality
Correct!	threat	data leakage
Correct!	value	sensitive
Correct!	vulnerability	rekeying

Question 2 — 1 / 1 pts

The one-time pad (OTP) cipher

Fix t to be any positive integer; set $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0,1\}^t$

- **Gen**: choose t bits uniformly at random (each bit independently w/ prob. .5)
  - Gen $\rightarrow \{0,1\}^t$
- **Enc**: given a key and a message of equal lengths, compute the bit-wise XOR
  - $\text{Enc}_k(m) = \text{Enc}_k(m) \rightarrow k \oplus m$ (i.e., mask the message with the key)
- **Dec**: compute the bit-wise XOR of the key and the ciphertext
  - $\text{Dec}(k, c) = \text{Dec}_k(c) := k \oplus c$
- Correctness
  - trivially, $k \oplus c = k \oplus k \oplus m = 0 \oplus m = m$

Recall the simple encryption scheme we saw in class - the One-Time Pad.

Is this cipher a symmetric-key or an asymmetric-key cryptographic scheme?

- Symmetric - because the key is randomly selected from the key space in a uniform manner.
- Symmetric - because above the XOR operation is applied bit-wise and not from left-to-right manner.
- Correct! Symmetric - because the same secret key is used both to encrypt and to decrypt.

Question 3 — 1 / 1 pts

Perfect secrecy (or information-theoretic security)

Definition 1

A symmetric-key encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$, is **perfectly secret** if for every $\mathcal{D}_M$, every message $m \in \mathcal{M}$ and every ciphertext $c \in \mathcal{C}$ for which $\Pr[C = c] > 0$, it holds that

$$\Pr[M = m \mid C = c] = \Pr[M = m]$$

In class we discussed the above definition for perfect secrecy. Which intuitive property does this definition capture?

- Correct! That by observing the ciphertext no additional information is revealed about the plaintext.

Question 4 — 1 / 1 pts

Alternative view of perfect secrecy

Definition 2

A symmetric-key encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$, is **perfectly secret** if for every messages $m, m' \in \mathcal{M}$ and every $c \in \mathcal{C}$, it holds that

$$\Pr[\text{Enc}_k(m) = c] = \Pr[\text{Enc}_k(m') = c]$$

Alternatively, we also discussed that perfect security for a symmetric-key encryption scheme (E, D) can be defined as above. What does this definition imply?

- That when the key K is chosen uniformly at random at set up, then any ciphertext c is equally likely the encryption of any two messages.
- That the search space of an attacker intercepting ciphertext c is reduced to a pair of plaintext messages, but the attacker cannot really tell apart which message is the encryption of c.
- Correct! That given a ciphertext c that is intercepted by an attacker, all possible plaintext messages are equally likely encrypted by c.

Question 5 — 1 / 1 pts

A given military base has a dedicated secure line for receiving/sending control messages of critical importance, e.g., commands from high-rank officers or status reports from soldiers in the battlefield. Messages are represented as 5-bit strings. Out of the 25 in total possible messages, 5 are rarely used (as they correspond to infrequent administrative procedures), whereas 7 of them are used in the majority of transmissions.

Suppose that one-time pad is correctly used to protect the message confidentiality. What describes the security of the transmission system?

- Correct! The system perfectly conceals the control messages because one-time pad is a perfectly secure cipher when it is correctly used.
- The system is insecure because the distribution of sent control messages is highly skewed so an attacker gains some knowledge about what messages a given ciphertext is likely to correspond to.
- The system is insecure because the small message lengths make the attacker's search space too small and thus susceptible to feasible brute-force attacks.

Question 6 — 1 / 1 pts

Unfortunately, if something is perfect in some aspect (in security), it must be weak in some other aspect (in usability). One-time pad is impractical, as a new secret key must be used any time Alice sends encrypts a new message.

Indeed, key reuse makes the scheme insecure. Consider the case where Alice uses the same secret key k to encrypt messages m_1 and m_2. What goes wrong in this case?

- Correct! The scheme is no longer perfectly secure because the XOR of the two transmitted messages can be learned.
- The scheme is insecure only when $m_1 = m_2$ (because in this case $c_1 = c_2$).
- The scheme may or may not become insecure depending on the quality of key k itself.

Question 7 — 1 / 1 pts

To protect the draft of the upcoming midterm exam m, suppose that I want to store it in my laptop encrypted as c = Enc(k,m), using some symmetric-key encryption scheme (Gen, Enc, Dec), where k is a secret key chosen from an appropriate key space uniformly at random. To further protect the key k, suppose that I do the following:

1) Using an appropriate second key k', I apply a one-time pad encryption on k to compute ciphertext c' = k XOR k'.

2) I give a USB drive storing c' to my TA Alice and a USB drive storing k' to my other TA Bob.

Alice seems a bit upset because she thinks that I don't trust her enough to give him the one-time pad key k', but only the ciphertext c'. Is she right to worry?

- Yes. The one-time pad key k' is more important to protect (and I happen to trust Bob slightly more).
- No. It is Bob really who should feel less trustworthy, as c' carries more information about the exam than k'.
- Correct! No. Both c' and k' are equally important pieces of information for the protection of the exam.