HW1

Problem R-1.17

$$P_{one\ bit\ English\ text} = \frac{number\ of\ English\ text}{total\ number} = \frac{2^{1.25}}{2^{8}} = \frac{1}{2^{6.75}}$$

$$P_{t-bit\ English\ text} = (P_{one\ bit\ English\ text})^{t} = (\frac{1}{2^{6.75}})^{t} = \frac{1}{2^{6.75*t}}$$

Problem R-1.18

Since the key is 32 bit, there will be 2^{32} possible keys and possible ways to decode.

$Number\ of\ ways\ to\ decode = total\ number * P_{t-bit\ English\ text} = 2^{32} * P_{t-bit\ English\ text}$

Using the probability in the previous.

$t = 8, Number\ of\ ways\ to\ decode = \frac{2^{32}}{2^{6.75*8}} = \frac{2^{32}}{2^{54}} = \frac{1}{2^{22}} < 1$

$t = 64, Number\ of\ ways\ to\ decode = \frac{2^{32}}{2^{6.75*64}} = \frac{2^{32}}{2^{432}} = \frac{1}{2^{400}} < 1$

$t = 512, Number\ of\ ways\ to\ decode = \frac{2^{32}}{2^{6.75*512}} = \frac{2^{32}}{2^{3456}} = \frac{1}{2^{3424}} < 1$

So the ciphertext will always be uniquely recovered for length 8, 64, 512 bytes.

Problem R-1.19

$Number\ of\ passwords = 128^{8}$

$Average\ time = 128^{8}/2\ nanoseconds = 1297\ hours$

Problem C-1.10

For message from Barack to Tim, it contains repetitive substring “How much to”, so the attacker could use this and guess part of the private key to decode $E_{pT}(m)$. Since the bank names are known and might have different lengths, the attacker can use that information to figure out the rest of the private key.

For messages from Tim to Barack, it contains mainly numbers and repetitive “$” and “B”, so the attacker can match “$” and “B” to the text first. For the rest of the ciphertext, it contains 10 numbers that sums up to $900B. The attacker can try a brute-force exhaustive search method and figure out the private key to decrypt $E_{pB}(r)$.

Problem C-1.11

As a result of the above attack, Barack decides to modify the protocol of Exercise C-1.10 for exchanging messages. Describe two simple modifications of the protocol that are not subject to the above attack. The first one should use random numbers and the second one should use symmetric encryption.

1. We can use an algorithm to generate random keys based on the time. In this case, the key for each message will be different, and the hacker will not be able to figure out the keys based on the message pattern.
2. We can set a set of symmetric keys and send each message encrypted with different symmetric keys.

Summary:
To summarize, an 18-year hacker used an automated password-guesser to gain access to a Twitter staff account because the password is too simple. Additionally, Twitter didn't set a lockout threshold after unsuccessful login attempts. This also made his attack easier. Then he used this account and a dictionary attack to gain access to the administrative Twitter account. He reset the password and posted on Digital Gangster, a forum for hackers, that he would share this account by request. The administrative account was shared to other hackers, who used it to post bogus messages, fake news, and phishing scams on the widely-trusted account.

In this attack, Twitter absolutely failed to set secure policies and provide protections with security principles, such as fail-safe default, separation of privileges, complete mediation, and least common mechanism. For the roles with more access to restricted resources, especially administrators, extra policies, authentication and protection should be enforced. For example, high-level password complexity, password rotation, and multi-factor authentication. As for complete mediation, there is almost no limit of failed attempts before the account is locked down. That means any account could be hacked by a brute-force exhaustive method if the hacker is given enough time. Even though one of the main goals of Twitter is sharing, the administrator accounts should be informed of the threads of oversharing. Personal information or even sensitive information could be accidentally shared and used in future malicious attacks.