HONEY CHATTING: A NOVEL INSTANT MESSAGING SYSTEM ROBUST TO EAVESDROPPING OVER COMMUNICATION

Joo-Im Kim and Ji Won Yoon / Center for Information Security Technologies (CIST), Korea University

ABSTRACT & INTRODUCTION

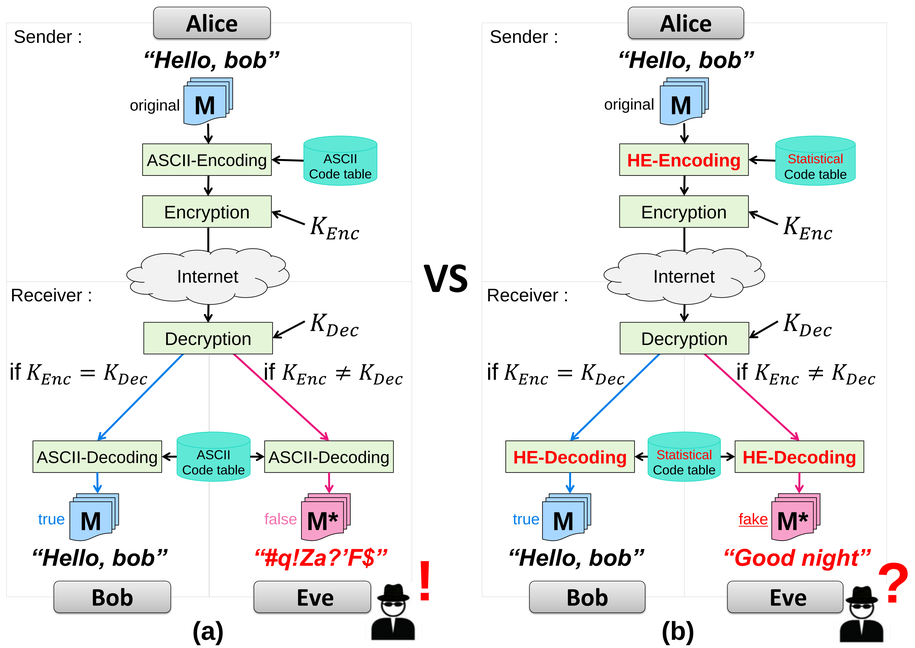
Secure Chatting

- To strengthen the security of *Instant Messaging* system, we typically encrypt messages. But the key for encryption has the potential vulnerability to be cracked by a brute-force attacker if its size isn't enough. So, we introduce a new concept of secure chatting by applying *Honey Encryption(HE)*, which makes it hard to distinguish the correctly decrypted text with a real key from decrypted texts with wrong keys.

Our Contribution

- Develop a Messaging system(Honey Chatting) robust to eavesdropping by using the concept of *HE*.
- Generate plausible-looking but fake plaintexts to confuse the brute-force attacker.
- Show the difference between a true message and fake messages by calculating the entropy of texts in the decrypted message.

STRUCTURE SUMMARY



Overall Procedure

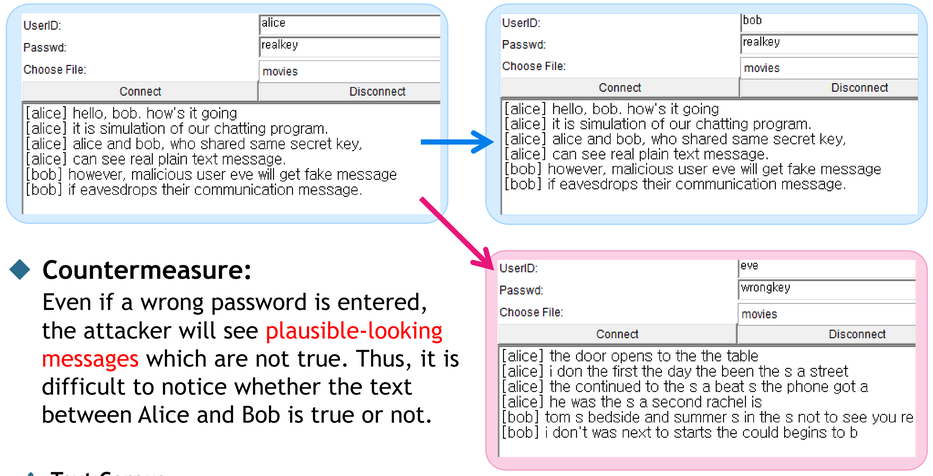
1) The sender's message **M** is encoded using the code table❖ and encrypted with K_{Enc}.
2) It passes through the communication channel such as the Internet.
3) The receiver decrypts it with K_{Dec} and decode it by using the same code table.
   If $K_{Enc} = K_{Dec}$, the receiver can obtain a true message **M** in both cases.
   Else If $K_{Enc} \neq K_{Dec}$, **M*** is become **false message in (a)** or **plausible-looking fake message in (b)**.

➔ **Therefore, Eve(brute-force attacker) is hard to find the true message.**

❖ Here, the **Statistical code table** is made from the statistical coding scheme using text corpus in advance, and the sender and the receiver share it.

HONEY CHATTING SIMULATION

Situation : While **Alice** and **Bob** enjoy chatting (share a real password), a malicious **Eve** is trying to eavesdrop their chat messages (try to enter passwords).



Countermeasure:

Even if a wrong password is entered, the attacker will see plausible-looking messages which are not true. Thus, it is difficult to notice whether the text between Alice and Bob is true or not.

❖ **Text Corpus**
We select text database such as movie subtitles or fictions including much dialogue rather than description in order to make fake messages to seem more like chat messages.

Statistical Coding Scheme

- Chat messages can be represented by N-gram language model, so we get the probability of consecutive characters in a sentence of message.
- We construct the cumulative massive function(CMF) based on the N-gram language model. CMF is used as statistical code table for HE-Encoding and HE-Decoding.
- The **CMF** for i-th character of message :

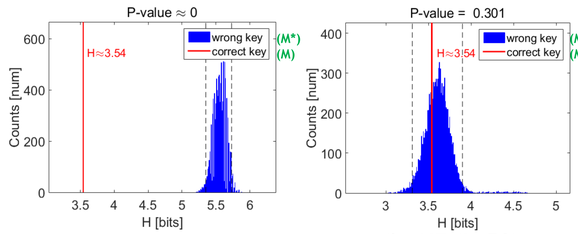
$$p_{\mathrm{cmf}}^{(\mathrm{i})}(c_k) = \sum_{k=0}^{S} \frac{p(x_i = c_k | \mathbf{x}_{i-1:i-n})}{\sum_{j=0}^{S} p(x_i = c_j | \mathbf{x}_{i-1:i-n})}$$

- S is the number of possible character set // *a~z, space, comma, period*
- n is the order of Markov process. // *n=5 in our application*
- $p(x_i|x_{i-1:i-n})$ is the i-th character influenced by previous n-1 characters

EXPERIMENT

The Difference of Entropy

- We conduct a significance test (hypothesis test) to show difference between decrypted text with wrong and real key when applying HE scheme.
- In **(a)**, P-value is significantly small which means there are clear distinction between **M** and **M***s. (**M**: true message, **M***: false or fake message)
- In **(b)**, moderately large P-value shows that observed data **M** is agreed with **M***s. It means that **M** is similar with **M***s, so the brute-force attacker could not notice his success.



(a) ASCII (L=50) (b) HE (L=50)

CONCLUSION

Summary

- Chatting systems enhance security by using message encryption, but it's still vulnerable to brute-force attack.
- We suggested a messaging system which is robust to eavesdropping.

Future Works

- For the practical use in the real world, we need to consider the context and grammar of messages.
- The available character set should be expanded. We used only 30 characters: letters(a-z), space, period, and comma.
- Consider other measures and experiment methods to prove the indistinguishability of decrypted messages.