COMP-547 2020 Homework set #2

Due Tuesday October 27, 2020, 23:59:59

Historic Cryptography

Exercises from Katz and Lindell's book (1.5, 1.11 (3rd ed.))

[10%] 1.5 Show that the shift, substitution, and Vigenère ciphers are all trivial to break using a chosen-plaintext attack. How much chosen plaintext is needed to recover the key for each of the ciphers?

[10%] 1.11 The attack on the Vigenère cipher has two steps: (a) find the key length by identifying τ with $S_\tau \approx 0.065$ (cf. Equation (1.3)) and (b) for each character of the key, find j maximizing I_j (cf. Equation (1.2)), using $\{p_i\}$ corresponding to English text. What happens in each case if the underlying plaintext is in a language other than English?

[5%] Refer to https://en.wikipedia.org/wiki/Letter_frequency for distributions of letters in 15 languages. Which of those 15 languages would be hardest to cryptanalyze, and why ?

Monogenère & Ligenère

Imagine that *Blaise de Vigenère* had used ***t*** mono-alphabetic substitutions instead of ***t*** shift ciphers to define his encryption scheme.

[5%] 1) Give a formal definition of the **Monogenère** encryption scheme.

[5%] 2) Explain why the methods we learned to break the **Vigenère** cipher are no longer sufficient to break the **Monogenère** encryption scheme.

[5%] 3) Explain however why we can still figure out the correct value of ***t***.

To be honest, I am not completely sure how we can break this system efficiently. So let me give you another one you can still break. Instead of pure mono-alphabetic substitutions, let's only generalize the simple shift cipher

$$c = m+k \bmod 26$$

to a somewhat more complicated cipher

$$c = e\cdot m+k \bmod 26$$

where the secret key is (***k***,***e***), 0 ≤ ***k***,***e*** ≤ 25, gcd(***e***,26)=1. This system has 312 possible key-pairs instead of 26. Let's call this a linear cipher. Similarly, let a **Ligenère** cipher be the system obtained by analogy to the **Vigenère** cipher using ***t*** independent linear ciphers instead of ***t*** independent shift ciphers.

[5%] 4) Define the decryption operation of a linear cipher with key-pair (***k***,***e***).

[10%] 5) How could we break the **Ligenère** cipher ? Give full details.

Perfect and Computational Secrecy

Let (Gen_1,Enc_1,Dec_1), (Gen_2,Enc_2,Dec_2), and (Gen_3,Enc_3,Dec_3) be three encryption schemes over the same message space $M=\{0,1\}^{\ell}$. Consider the composite scheme (Gen_c,Enc_c,Dec_c) over message space $M=\{0,1\}^{\ell}$ defined as

Gen_c = (Gen_1,Gen_2,Gen_3)

$Enc_c(m)$ = **pick** uniformly at random u,v $\in$ M, independently from m;
return ($Enc_1(u)$, $Enc_2(v)$, $Enc_3(u \oplus v \oplus m)$)

$Dec_c(x,y,z)$ = **return** ($Dec_1(x) \oplus Dec_2(y) \oplus Dec_3(z)$)

[10%] Prove that if any of the three encryption schemes (Gen_s,Enc_s,Dec_s), $1 \le s \le 3$, is *perfectly secret* then so is (Gen_c,Enc_c,Dec_c).

Exercise from Katz and Lindell's book **(2.10 (3rd ed.), 3.2, 3.3)**

2.10 The following questions concern the message space $\mathcal{M} = \{0,1\}^{\le \ell}$, the set of all nonempty binary strings of length at most ℓ.

[5%] (a) Consider the encryption scheme in which Gen chooses a uniform key from $\mathcal{K} = \{0,1\}^{\ell}$, and $\mathsf{Enc}_k(m)$ outputs $k_{|m|} \oplus m$, where k_t denotes the first t bits of k. Show that this scheme is not perfectly secret for message space $\mathcal{M}$.

[10%] (b) Design a perfectly secret encryption scheme for message space $\mathcal{M}$.

[10%] 3.2 Prove that Definition 3.8 cannot be satisfied if Π can encrypt arbitrary-length messages and the adversary is *not* restricted to outputting equal-length messages in experiment $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$.

Hint: Let $q(n)$ be a polynomial upper-bound on the length of the ciphertext when Π is used to encrypt a single bit. Then consider an adversary who outputs $m_0 \in \{0,1\}$ and a uniform $m_1 \in \{0,1\}^{q(n)+2}$.

[10%] 3.3 Say $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is such that for $k \in \{0,1\}^n$, algorithm Enc_k is only defined for messages of length at most $\ell(n)$ (for some polynomial ℓ). Construct a scheme satisfying Definition 3.8 even when the adversary is *not* restricted to outputting equal-length messages in $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$.