Lecture 14 Outline

May 12, 2016

Reading: *text*, §10 **Assignments due:** Homework 3, on May 12

1. Greetings and felicitations!
   a. Discussion question
2. Symmetric Cryptography
   a. Monoalphabetic (simple substitution): $f(a) = a + k \bmod n$
   b. Example: Caesar with $k = 3$, RENAISSANCE → UHQDLVVDQFH
   c. Polyalphabetic: Vigenère, $f_i(a) = a + k_i \bmod n$
   d. Cryptanalysis: first do index of coincidence to see if it is monoalphabetic or polyalphabetic, then Kasiski method.
   e. Problem: eliminate periodicity of key
3. Long key generation
   a. Autokey cipher:
      M = `THETREASUREISBURIED`
      K = `HELLOTHETREASUREISB`
      C = `ALPEFXHWNIIIKVLVQWE`
   b. Running-key cipher:
      M = `THETREASUREISBURIED`
      K = `THESECONDCIPHERISAN`
      C = `MOILVGOFXTMXZFLZAEQ`
      wedge is that (plaintext, key) letter pairs are not random (T/T, H/H, E/E, T/S, R/E, A/O, S/N, etc.)
   c. Perfect secrecy: when the probability of computing the plaintext message is the same whether or not you have the ciphertext
   d. Only cipher with perfect secrecy: one-time pads; C = `AZPR`; is that `DOIT` or `DONT`?
4. Product ciphers: DES, AES
5. Public-Key Cryptography
   a. Basic idea: 2 keys, one private, one public
   b. Cryptosystem must satisfy:
      i. Given public key, computationally infeasible to get private key;
      ii. Cipher withstands chosen plaintext attack;
      iii. Encryption, decryption computationally feasible (*note*: commutativity not required)
   c. Benefits: can give confidentiality or authentication or both
6. Use of public key cryptosystem
   a. Normally used as key interchange system to exchange secret keys (cheap)
   b. Then use secret key system (too expensive to use public key cryptosystem for this)
7. RSA
   a. Provides both authenticity and confidentiality
   b. Go through algorithm:
      Idea: $C = M^e \bmod n$, $M = C^d \bmod n$, with $ed \bmod \phi(n) = 1$
      Public key is (e, n); private key is d. Choose $n = pq$; then $\phi(n) = (p-1)(q-1)$.
   c. Example: $p = 5$, $q = 7$; then $n = 35$, $\phi(n) = (5-1)(7-1) = 24$. Pick $d = 11$. Then $ed \bmod \phi(n) = 1$, so $e = 11$
      To encipher 2, $C = M^e \bmod n = 2^{11} \bmod 35 = 2048 \bmod 35 = 18$, and $M = C^d \bmod n = 18^{11} \bmod 35 = 2$.
   d. Example: $p = 53$, $q = 61$; then $n = 3233$, $\phi(n) = (53-1)(61-1) = 3120$. Pick $d = 791$. Then $e = 71$
      To encipher M = `RENAISSANCE`, use the mapping `A = 00`, `B = 01`, ..., `Z = 25`, b̸ = 26.
      Then: M = `RE NA IS SA NC Eb̸` = 1704 1300 0818 1800 1302 0426
      So: $C = (1704)^{71} \bmod 3233 = 3106; \ldots = 3106\ 0100\ 0931\ 2691\ 1984\ 2927$

Discussion question. An eighth grade school student in Florida shoulder-surfed a teacher he didn't like typing in a password. He used that password to log into the teacher's account and changed the wallpaper. The password, like all passwords on the school network, was the last name of the teacher (user), and teachers had administrative privileges on the network.

The student was first suspended for 10 days. But on April 2, 2015, the Pasco County sheriff filed felony charges against the student. The sheriff stated that he filed the charges because the teacher's computer had "encrypted 2014 FCAT [Florida Comprehensive Assessment Test] questions", although he admitted the student "did not view or tamper with those files." He added "Even though some might say this is just a teenage prank, who knows what this teenager might have done."

Do you think the student should have been suspended? Should he have been charged with a felony?