Zizhong Zhu
z63zhu
20530820

Assignment 3

- 1. **Cryptosystems**
  - (a) OTP
    - i. C1 = P1 ⊕ K, C2 = P2 ⊕ K, C1 ⊕ C2 = P1⊕K⊕P2⊕K = (P1 ⊕ P2) ⊕ (K⊕K) = P1 ⊕ P2 because for any string XOR it self equal to 0. e.g: P1 = 1011, P2 = 1001, k = 1111, so C1 = 0100, C2 = 0110, C1 ⊕ C2 = 0010, P1⊕P2 = 0010, so P1⊕P2 = C1⊕C2.
    - ii. Use "crib-dragging" technique, which use a list of common words and space in message, XOR each words to P1 ⊕ P2, if the result looks like readable English message, the word we try could be right, and the result would be right for another message. Use a program do it until we got a whole message.
    - iii. Yes, can determine K by C1 ⊕ P1 = P1 ⊕ K ⊕ P1 = (P1 ⊕ P1) ⊕ K = K
  - (b) RSA
    - i. This scheme secure cannot against replay attacks, can be prevented by tagging each encrypted component with a session ID and a component number. Eve cannot do the replay attack because the session ID would change each time.
    - ii. It depends on the n, M=C^d mod n, d * e = 1 mod ϕ(n), n=p * q, ϕ(n)=(p-1)(q-1), if the n is not large enough, the p and q would be computed by eve, then they can use p,q to calculate d which is e*d = 1 mod ϕ(n) , then can decrypt the message, so if the n is large enough, then attacker cannot recover the plaintext.
    - iii. Can use Hybrid cryptography, when decrypt the key provide by sender, the key can authenticate the sender, also can add timestamps or nonces to defend replay attack.

- 2.**GnuPG**
  - (d) Fingerprints can help user verify the key they receive is what they want. The first condition is it can prevent Eve make fake key to receivers, attackers can make fake keys but they cannot counterfeit the keys with right fingerprints; another condition is when user wanna receive others keys, it has possibility to have keys with same user name, email and other parameters, at this time, the fingerprint would determine which key is the key you wanna download.

- 3. **Data Privacy**
  - (a)[2k : N-2k] => [0.1N~0.4N : 0.6N~0.9N]
    - Tracker = SELECT SUM(Salary) FROM Employee WHERE Type = "nurse"
    - Tracker will be 0.6N which would match [2k : N-2K]
    - Q1 = SELECT SUM(Salary) FROM Employee WHERE Type = "Nurse" OR ID = "jdoe"
    - Q2 = SELECT SUM(Salary) FROM Employee WHERE Type != "Nurse" OR ID = ""jdoe"
    - Q3 = SELECT SUM(Salary) FROM Employee WHERE Type != "Nurse"

- Salary of “jdoe” = Q1 + Q2 - T - Q3
- (b)

Age	Gender	Disease
65	M	Heart disease
65	M	Flu
65	M	Heart disease
65	M	Cancer
78	M	Heart disease
78	M	Alzheimer’s
78	M	Heart disease
79	F	Flu
79	F	Heart disease
79	F	Cancer
79	F	Cancer

It is 2-diverse.

Application Description

- (1). worst case: O(NbW), average case is O(NbW/2)
  - b: if last block only has 1 bit text and b-1 paddings
  - N: need to decrypt N times (1 for each block)
  - W: W is the number of possible words(typically W = 256)

- (2) can use Encrypt-then-MAC to fix this vulnerability, The cipher text is generated by encrypting the plaintext and then appending a MAC of the plaintext. This is approximately how SSH works, it can provide:
  - Confidentiality: attacker can not decrypt
  - Authenticity: attacker can not encrypt

- (3)The first byte of the padding has the 0x01, and all other padding bytes have the value 0x00
  - 3.1: change line **5** (b) to:
    (b) if O(rly)=0 then stop and output ($r_{b-n+1} \oplus \mathbf{1}$) ($r_{b-n+2} \oplus \mathbf{0}$)…($r_b \oplus \mathbf{0}$)
  - 3.2: change **Line 1 and Line 5** to:
    - (1) take $r_k = a_k \oplus 0$ for k=j,…,b
    - (5) output $r_{j-1} \oplus i \oplus 1$