COMP4334 Homework 1

1.1 Security under different threat models

Answer:

The DH Key Exchange can prevent the eavesdroppers from getting, but can not prevent the man-in-the-middle attack. Because the DH Key Exchange uses shared info and its own private key to compute, it is difficult to compute by a third person. But in the exchange period, the third person can create 2 keys to change or alter.

1.2 Randomness in encryption

Answer:

In the ElGamal encryption if re-use the random number `k` to encrypt 2 different messages, the attacker which can compute by division, if attacker know the one of the message, so user can use that key stream to get another message. For example:

```
A = (A1, A2) = (a^k mod q, (YA)^k * m1 mod q)
B = (B1, B2) = (a^k mod q, (YA)^k * m2 mod q)

A2 / B2 = m1 / m2 mod q

m1 known
m2 can be compute
```

1.3 Public key distribution

Answer:

If everyone write the public key on the board, so the attacker can just change the public key to attacker's public key, and let other people to use attacker's public key, when attacker get the cipher text, attacker can decrypt it.

---

2 Operation Modes of Block Ciphers

(a) Answer

If before encryption, one bit of the tenth plaintext block is modified, so there will be have 9 blocks (before 10th) can decrypt correctly, other blocks will be broken.

(b) Answer

If after encryption, one bit of the tenth ciphertext block is changed, because of the CBC mode feature, use the cipher text which from encrypt previous block to be the random number add into the next block encryption. So only the 10th, and 11th will be affected.

---

3 Secret Dating

1 Answer

Alica ask question, Bob reply: Alica encrypted message size > Bob encrypted reply size

Because the time length is 24h format, is fixed, so can get location length easily.

Also, if have some part is same, so the text is same, if the front of the cipher text is same, so they already make sure the location, and time is same.

2 Answer

To prevent people from knowing the dating plan, Bob can add some random data to the reply, use only Yes or No, but can add some random padding in the end.

4 Attacks against Textbook RSA

1 Answer

Use RSA public key to encrypt 128 bits message is a bad idea, because the message is smaller than n, this may cause the brute force attack, and easy to decrypt the message.

Alica can use padding, to ensure the message size is larger than n or enough relative to n, can improve the security.

2 Answer

Eve can use extended Euclidean theorem, because of the eA = 3, eB = 5,

```
CA = m^eA mod n = m^3 mod n
CB = m^eB mod n = m^5 mod n

gcd(3, 5) = 1
m^3 = CA mod n
m^5 = CB mod n

3x + 5y = 1
(CA^x *CB^y) mod n = (m^3x * m^5y) mode n = m^1 mod n = m
```

So, the Eve can recover the message m from CA, CB, and n.

3 Answer

3 Public Key: `(e1 = 3, N1)`, `(e2 = 3, N2)`, `(e3 = 3, N3)`

3 Cipher Text: `C1 = m^3 mod N1`, `C2 = m^3 mod N2`, `C3 = m^3 mod N3`,

According to the Chinese Reminder Theorem

```
x ≡ C1 mod N1
x ≡ C2 mod N2
x ≡ C3 mod N3

x = m^3 mod (N1 * N2 * N3)
```

Also, N1, N2, N3 are pairwise prime, so the N1 * N2 * N3 will be bigger than m^3.

So, the x = m^3, m = cube root of x

---

5 Cryptographic Hash Function

1 Answer

```
H(x ⊕ y) = H(x) ⊕ H(y)
H: {0, 1}^* -> {0, 1}^n

x = 0^k
x ⊕ 0^k = x

H(0^k) = 0^n
```

2 Answer

H is not strong-collision resistant becasue of we can easily to find the same hash value, because of `H(y) = 0^n`, that `x or x' = x ⊕ y`

```
H(x ⊕ y) = H(x) ⊕ H(y)
x' = x ⊕ y
H(x') = H(x ⊕ y)

According to H(x ⊕ y) = H(x) ⊕ H(y) = H(x')
If have a collision: H(x') = H(x)
H(x) = H(x) ⊕ H(y)
H(y) = 0^n
```