VE475 Homework7

Anna Li
Student ID: 518370910048

Ex. 1 — Cramer-Shoup cryptosystem

1.

The encryption algorithm:
After Bob sends Alice plaintext m, Bob maps m to an element of G. Then he chooses a random number r which is $0 \leq r \leq p-1$. Last Bob calculates $u_1 = g_1^r$, $u_2 = g_2^r$, $e = h^r m$, $a = H(u_1, u_2, e)$ and $v = e^k d^{aR}$. Then ciphertext is c= (u_1, u_2, e, v).
The decryption algorithm:
If $u_1^{x_1+ay_1} u_2^{x_2yy_2a} = v$, the plaintext m would be $\frac{e}{u_1^z}$. The decryption will fail in other way.
The generation of the key algorithm:
After a cyclic group G with order p is generated by Alice, she finds two key generators g1 and g2 for G. Alice chooses x_1, x_2, y_1, y_2, zwhich in $\{1, 2, ..., p-1\}$ and computes ciphertext$g_1^{x_1}$,$g_2^{x_2}$, d=$g_1^{y_1} g_2^{y_2}$, h=g_1^z. H is a one-way trapdoor function be generated. Lastly, private keys are x_1, x_2, y_1, y_2, z and c,d,h,G,p,g_1, g_2 are public keys.

2.

CCA could be used. Because the attackers could attack by conducting different ciphertexts. However, the decryption algorithm doesn't allow all ciphertexts because of one way collision-resistant hash function.

3.

Similarity
Calculation is in symmetric group is both hard to decrypt due to discrete logarithm problems.
Difference:
Another protecting layer is added for Cramer algorithm (trpdoor one-way hash function). Moreover, it can restrict the input of cipher. Therefore, Cramer-Shoup system is safer.

Ex. 2 — Simple questions

1.

If p is a prime and p $\not|\alpha$,which means gcd(p,α)=1 and we can get $\alpha^{p-1} \equiv 1 \mod p$ by Euler's theorem. Since the hash function isn't second pre-image resistant, since x is known, we can find $x' = x + (p-1)$ and $h(x) = h(x')$, which is not collision resistant too. Therefore it's not a good cryptographic hash function.

2.

$$2^{30} = 0x40000000$$
$$\Rightarrow floor(2^{30} * \sqrt{2}) = 5A827999$$
$$\Rightarrow floor(2^{30} * \sqrt{3}) = 6ED9EBA1$$
$$\Rightarrow floor(2^{30} * \sqrt{5}) = 8F1BBCDC$$
$$\Rightarrow floor(2^{30} * \sqrt{10}) = CA62C1D6$$

Therefore, the result is the same as $K_0||......||K19, K20||......||K39, K40||......||K59andK60||......||K79.$

Ex. 3 — Birthday paradox

1.

$$g(x) = ln(1-x) + x + x2$$
$$\Rightarrow g'(x) = -\frac{1}{1-x} + 1 + 2x$$

When x=0 or 0.5⇒g'(x)=0

$$\Rightarrow g''(x) = -\frac{1}{x-1}^{2} + 2$$

Therefore, g(0)=1 is local min, g(0.5)=-2 is local max.
When $x \in [0, 0.5]$, $g(x) \in [g(0), g(0.5)] >= 0$
Similarly, we set h(x) = ln(1 - x) + x

$$\Rightarrow h(x) \in [g(0.5), g(0)] <= 0$$

Therefore, $-x - x^2 <= ln(1-x) <= -x$

2.

$j \in [1, r-1]$ and $r \le \frac{n}{2} \Rightarrow \frac{j}{n} \in \left[0, \frac{1}{2}\right]$

$$\Rightarrow -\frac{j}{n} - \left(\frac{j}{n}\right)^2 \le \ln\left(1 - \frac{j}{n}\right) \le -\frac{j}{n}$$

$$\Rightarrow \sum_{j=1}^{r-1}\left[-\frac{j}{n} - \left(\frac{j}{n}\right)^2\right] \le \sum_{j=1}^{r-1}\ln\left(1 - \frac{j}{n}\right) \le \sum_{j=1}^{r-1} -\frac{j}{n}$$

$$\Rightarrow -\frac{(r-1)r}{2n} - \frac{(r-1)r(2r-1)}{6n^2} \le \sum_{j=1}^{r-1}\ln\left(1 - \frac{j}{n}\right) \le -\frac{(r-1)r}{2n}$$

When $r > 1$,
$\frac{(r-1)r(2r-1)}{6n^2} = \frac{r^3 - \frac{3}{2}r^2 + r}{3n^2} < \frac{r^3}{3n^2}$
Therefore,
$-\frac{(r-1)r}{2n} - \frac{r^3}{3n^2} \le \sum_{j=1}^{r-1}\ln\left(1 - \frac{j}{n}\right) \le -\frac{(r-1)r}{2n}$

3.

$$\exp\left(-\frac{(r-1)r}{2n} - \frac{r^3}{3n^2}\right) \le \prod_{j=1}^{r-1}\left(1 - \frac{j}{n}\right) \le \exp\left(-\frac{(r-1)r}{2n}\right)$$

Supposing $\lambda = \dfrac{r^2}{2n}$,

$$c_1 = \sqrt{\frac{\lambda}{2}} - \frac{(2\lambda)^{3/2}}{3}$$

$$c_2 = \sqrt{\frac{\lambda}{2}}$$

$$\Rightarrow -\lambda + \frac{c_1}{\sqrt{n}} = -\frac{r^2}{2n} + \frac{r}{2n} - \frac{r^3}{n^2} = -\frac{(r-1)r}{2n} - \frac{r^3}{3n^2}$$

$$\Rightarrow -\lambda + \frac{c_2}{\sqrt{n}} = -\frac{r^2}{2n} + \frac{r}{2n} = -\frac{(r-1)r}{2n}$$

Therefore,

$$e^{-\lambda}e^{c_1/\sqrt{n}} \le \prod_{j=1}^{r-1}\left(1 - \frac{j}{n}\right) \le e^{-\lambda}e^{c_2/\sqrt{n}}$$

4.

When n is large and $\lambda = \frac{r^2}{2n} < \frac{n}{8}$, $r < \frac{n}{2}$
Since λ is constant, c_1 and c_2 are all constants.

$$\Rightarrow \lim n -> \inf e^{\frac{c_1}{\sqrt{n}}} = 1$$

$$\Rightarrow \lim n -> \inf e^{\frac{c_2}{\sqrt{n}}} = 1$$

Therefore, we can get: $\sum_{j=1}^{j=r-1}(1 - \frac{j}{n}) = e^{-\lambda}$

Ex. 4 — Birthday attack

1.

0.546

2.

0.039

3.

It's easy to find a collision in a hash function, and it's hard to find a collision of a specific massage. This means that Alice could overcome the problem by changing a bit in the massage but Eve cannot find a collision of new massage easily.

Ex. 5 — Faster multiple modular exponentiation