CS427. HW 2.

Zongyan Lu

1. 2-out-of-10 Shamir Secret sharing.

Z_{11}.

Alice (4,6).

Bob (7,3).

Based on the definition.

we get point (4,6) (7,3)

$$\Rightarrow \begin{cases} (4, f(4)) = (4,6) \\ (7, f(7)) = (7,3) \end{cases}$$

$y = kx+b$

$$\Rightarrow \begin{cases} 6 = 4k+b \\ 3 = 7k+b \end{cases} \Rightarrow \begin{cases} k = -1 \\ b = 10 \end{cases}$$

So. the Secret equation it constructed:

$y = -x+10$

And other 8 shares:

- $S_1 = 9$.
- $S_2 = 8$
- $S_3 = 7$
- ($S_4 = 6$) already know.
- $S_5 = 5$
- $S_6 = 4$
- ($S_7 = 3$) already know
- $S_8 = 2$
- $S_9 = 1$
- $S_{10} = 0$

3. last 4 digit Student ID. assigned uniformly.

Total 46 students.

$Pr[$ Student$_1$ last 4 digit = Student$_2$ [last 4 digit] $= ?$

For a digit. $0 \sim 9$.

Assume the event as A.

So. $\bar{A}$ is two students have not identical last 4 digit.

$$P(\bar{A}) = \frac{9999}{10^4} \times \frac{9998}{10^4} \times \cdots \times \frac{9954}{10^4}$$

total possibility

total 46 students

$\therefore P(A) = 1 - P(\bar{A})$.

2. If p is non-prime.

Assume $p = 255$ $(1 \times 3 \times 5 \times 17)$.

Suppose $k=2$, shares: $\{(1,0), (4,0)$

Set a linear equation set: $ch_0 + s = 0$

4·a+5=0.

For library. $\mathbb{Z}_{257}$.

which $P=\{(1,0),(4,0)\}\subseteq(\mathbb{Z}_{257})^{\sim}$

we can get $f(x)=0x+0$

$f(x)=85x+170$

$f(x)=170x+85$.

three possible equations.

Hence, we know the secret is one of 0, 85, 170.

from possible equations by modulo 257.

But we can't identify the specific one of that.

So. the non-prime p shall break the claim to generate more than one degree-d polynomial.

4. 2^{128} pw for brute force

a). pw. lowcase a through z. only

1 digit: 26 possibility.

2 digit: $26\times26=26^2$ possibility

⋮

n digit: $(26)^n$ possibility.

So. $(26)^n > 2^{128}$

take lg for both side.

$\lg 26^n > \lg 2^{128}$

$\Rightarrow n\lg 26 > 128\cdot\lg 2$

b) pw. lowcase a-z and A-Z

1 digit: 52 possibility

2 digit: $(52)^2$ possibility

⋮

n digit: $(52)^n$ possibility.

So. $(52)^n > 2^{128}$

take lg for both side.

$\lg(52)^n > \lg 12^{128}$

$\Rightarrow n\cdot\lg 52 > 128\cdot\lg 2$

$\Rightarrow n > 128\cdot\frac{\lg 2}{\lg 52}$

$\Rightarrow n > 128 \cdot \frac{\lg 2}{\lg 26}$

$\Rightarrow n > 27.2$

$\Rightarrow n \geq 28$

So. at least 28 digits character long of this password to enforce pw rules.

c). pw lower/upper letters and digits 0-9

1. digit possibility: $26+26+10) = 62$.

2 digits possibility: $(62)^2$

⋮

n digits possibility: $(62)^n$

So. $(62)^n > 2^{128}$

take lg for both side.

$\lg (62)^n > \lg 2^{128}$

$n \cdot \lg 62 > 128 \lg 2$

$n > 128 \cdot \frac{\lg 2}{\lg 62}$

$n > 21.497$

$n \geq 22$.

So, at least 22 character long of this password to enforce pw rules.

$\Rightarrow n > 22.454$

$\Rightarrow n \geq 23$.

So. at least 23 digits character long of this password to enforce pw rules.

d). pw lower/upper letters, digits, any symbol appear on a standard US keyboard.

a-z 26.
A-Z 26.
0-9 10.
} $\Rightarrow 92$.
rest symbols: 30.

1 digit possibility: 92

2 digits possibility: $(92)^2$

⋮

n digits possibility: $(92)^n$

So. $(92)^n > 2^{128}$

$n \cdot \lg 92 > 128 \cdot \lg 2$

$n > 128 \cdot \frac{\lg 2}{\lg 92}$

$n > 19.621$

$n \geq 20$

So, at least 20 character long of this password to enforce pw. rules.