Assignment1 2230016081 Zhou Le

1.

(a)

1) The economic mechanism of open source is to make money by sharing code for free and reusing scale. Developers increase their technical capital and community reputation by contributing code, while enterprises reduce development costs through open source and make money through value-added services.
2) For individual incentives, open source contributions boost developers' technical credit and make it easier for them to be recruited by large enterprises. In addition, developers can obtain stable profits through the value-added services of the project. For Corporate Incentives, collaborative development can reduce the cost of R&D and become a market leader
3) Open source will certainly become a core business model, and GitLab statistics show that open source projects are three times more effective at converting enterprise customers than traditional sales, demonstrating that open source has become the foundation of business in the digital age. In addition, open source has become a globally collaborative approach to code production, greatly improving global productivity.

(b)

1) Tech Anarchy is a system of technological philosophy and practice that emphasises decentralisation, free collaboration and anti-authoritarianism, with its core proposition being the dismantling of traditional power structures through technological means and the creation of self-organising systems that do not require trusting intermediaries.
2) Blockchain, as an experiment in technological anarchism, proves the feasibility of code autonomy, but also exposes problems of recentralisation of rights, regulatory countermeasures and anonymisation of crime.

(c)

1) Both are essentially faced with the impossible triangle of ‘fairness, efficiency and stability’, and solutions in reality tend to be mixed models. Democratic voting may generate a cycle of contradictions, making collective decision-making unable to achieve stable results. The market mechanism is difficult to aggregate real preferences, bringing about irrational market behaviours and information cocooning.
2) Improvements can be made, but there is no way to break through the fundamental limitations, and only a mix of ‘technology + system’ can solve the problem. Blockchain can improve voting

transparency, smart contracts can automatically enforce rules, AI and big data can assist in analyses, they can improve efficiency, but they cannot solve the problem of ‘impossibility of perfect decision-making’ revealed by Arrow's theorem.

2.

(a)

$0 * 2^{11} + 1 * 2^{10} + 0 * 2^{9} + 1 * 2^{8} + 1 * 2^{7} + 0 * 2^{6} + 1 * 2^{5} + 1 * 2^{4} + 1 * 2^{3} + 1 * 2^{2} + 1 * 2^{1} + 0 * 2^{0}$

$= 0 + 1024 + 0 + 256 + 128 + 0 + 32 + 16 + 8 + 4 + 2 + 0$

$= (1470)_{10}$

(b)

$((0101)_2)_{16}$ =5

$((1011)_2)_{16}$ =B

$((1110)_2)_{16}$ =E

so 010110111110_2=$(5BE)_{16}$

(c)

1470/16 = 91……14=E_{16}

91/16=5……11=B_{16}

5/16=0……5

So 1470_{10}=$(5BE)_{16}$

3.

(a)

(44+33) mod 57= 20

(9-29) mod 57= 37

(b)

(95 · 45 · 31) mod 97=132,525 mod 97= 23

(17 · 13 · 19 · 44) mod 97=184,756 mod 97 = 68

(c)

31 is prime, so $b^{-1} = b^{31-2} = b^{29}$

$\frac{3}{24} = 3 * 24^{-1} = (3 * 24^{29}) \bmod 31 = 318601095192201503284717287408635970846 72 \text{mod}\ 31 = 4$

$17^{-3} = 17^{-1} * 17^{-1} * 17^{-1} = 17^{29*3}\ \%\ 31$

$= 1119582650665875945846132488928120136974866866692599679184071749784554112565256770753988635891994427679258 73\ \%\ 31 = 29$

4.

(a)

Y_A=(5^{15} mod 157)= 30517578125 mod 157 = 79

(b)

Y_B=(5^{27} mod 157)= 7450580596923828125 = 65

(c)

K_A = 65^{15} mod 157=156206948895540640258789 0625 mod 157 = 78

K_B = 79^{27} mod 157=1721596871731553058546849392211992003843558871355759 mod 157 = 78

So the shared secret key is 78

5.

(a)

C_1=5^3 mod 157 = 125

S=10^3 mod 157 = 58

C_2= (9*58) mod 157 = 522 mod 157 = 51

So the ciphertext is (125, 51)

(b)

Assume integer k, we get 5^k mod 157 = 25, then k = 2

S = 10^2 mod 157 = 100

C_2 = 9*100 mod 157 = 115

6.

(a) Signature Generation

1. *input*: large prime number $\mathbf{p}$, primitive root $\boldsymbol{\alpha}$, private key $\mathbf{x}$, public key $(\mathbf{p}, \boldsymbol{\alpha}, \boldsymbol{\beta})$, message $\mathbf{m}$ $(0 \leq \mathrm{m} < \mathrm{p})$. Randomly select $\mathbf{k}$ $(1 < \mathrm{k} < \mathrm{p} - 2$ and $\gcd(\mathrm{k}, \mathrm{p} - 1) = 1)$.

2. *Calculation*

Step1. compute

$$\mathbf{r} = \boldsymbol{\alpha}^{\mathbf{k}} \,\mathbf{mod}\, \mathbf{p}$$

Step2. compute

$$\mathbf{s} = \mathbf{k}^{-1}(\mathbf{m} - \mathbf{xr}) \,\mathbf{mod}\, (\mathbf{p} - \mathbf{1})$$

where k^{-1} is the multiplicative inverse of k modulo $(\mathrm{p} - 1)$.

3. *Output*: The final signature is $(\mathbf{r}, \mathbf{s})$

(b) Signature Verification

1. *Input*: The received message $(\mathbf{m}, \mathbf{r}, \mathbf{s})$, public key $(\mathbf{p}, \boldsymbol{\alpha}, \boldsymbol{\beta})$

2. *Calculation*:

Step1. Compute

$$\boldsymbol{\beta}^{\mathbf{r}}\mathbf{r}^{\mathbf{s}} \,\mathbf{mod}\, \mathbf{p}$$

Step2. compute

$$\boldsymbol{\alpha}^{\mathbf{m}} \,\mathbf{mod}\, \mathbf{p}$$

3. *Output*:

If $\boldsymbol{\beta}^{\mathbf{r}}\mathbf{r}^{\mathbf{s}} = \boldsymbol{\alpha}^{\mathbf{m}} \,\mathbf{mod}\, \mathbf{p}$ holds

the signature is valid; otherwise, the signature is invalid.

(c)

1. Signature Generation

set $\mathbf{p} = 17$, $\boldsymbol{\alpha} = 7$, $\mathbf{x} = 3$

∴ public key $\boldsymbol{\beta} = 7^3 \bmod 17 = 343 \bmod 17 = 3$

set message $\mathbf{m} = 6, \mathbf{k} = 5$

∴ $\mathbf{r} = 7^5 \bmod 17 = 16807 \bmod 17 = 11$, $\mathbf{s} = 13 * (6 - 3 * 11) \bmod 16 = 1$

∴ the signature for message **m**=6 is (11,1)

2. verification of signatures:

Take $\boldsymbol{\beta}^{\mathbf{r}}\mathbf{r}^{\mathbf{s}} \,\boldsymbol{mod}\, \boldsymbol{p}$ as LHS, $\boldsymbol{\alpha}^{\mathbf{m}} \,\mathbf{mod}\, \mathbf{p}$ as RHS,

LHS= $3^{11}11^1 \bmod 17 = 1948617 \bmod 17 = 9$

RHS= $7^6 \bmod 17 = 117649 \bmod 17 = 9$

Because LHS=RHS, so this signature is valid.

7.

(a)

Zero-knowledge proofs is a way to prove something without revealing unnecessary information

In cryptography, a zero-knowledge proof or zero-knowledge protocol is a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true, while avoiding conveying to the verifier any information beyond the mere fact of the statement's truth.

(b)

1. *Parameters:*

k: the security parameter (number of rounds)

σ: a random permutation on V_0

b ∈ {0,1}: the verifier's challenge bit

2. *input:*

Common input: Two graphs $\mathbf{G_0=(V_0,E_0)}$, $\mathbf{G_1=(V_1,E_1)}$ (with $|V_0|=|V_1|=n$)

Prover's private input: A permutation $\boldsymbol{\pi}: \mathbf{V_0} \rightarrow \mathbf{V_1}$ such that $\mathbf{G_1} = \boldsymbol{\pi}(\mathbf{G_0})$

Security parameter: **k** (number of rounds)

Step1: initialization

The Prover (P) and Verifier (V) agree on G_0, G_1

P knows π, V does not.

Step2: Interactive Phase (Repeated k times)

For each round: $\mathbf{i} \in \{\mathbf{1}, \dots, \mathbf{k}\}$

1. Prover selects a random permutation **σ∈** $\mathbf{S_n}$, Computes $\mathbf{H=\sigma(G_0)}$, Sends H to Verifier
2. Verifier selects a random challenge bit **b** ← **{0,1},** Sends b to Prover
3. Prover responds with:

If b=0, Prover sends $\boldsymbol{\phi} = \boldsymbol{\sigma}$**;**

If b=1, Prover sends **ϕ=σ∘π−1;**

4. Verifier checks if

$$\mathbf{H} = \boldsymbol{\phi}(\mathbf{Gb}),$$

If check fails, protocol terminates with rejection

Step 3: Verification

If all k rounds pass verification, V accepts the proof. If any round fails, V rejects.

(c)

ZKP alone cannot defend against man-in-the-middle attacks because ZKP functions to complete proof of knowledge without revealing any additional information and does not involve communication security. In the underlying ZKP protocol, a man-in-the-middle can steal information, or tamper with it, by posing as a verifier or impersonating a prover. If you need to defend against man-in-the-middle attacks, additional encryption is necessary.