Topics to remember

- Probability
  - Birthday Paradox: 1 − P(nobody has a common birthday) and $1-\frac{k}{d} < e^{-k/d}$
  - Random Variables:
    - Binomial: $P(X=k) = \binom{n}{k} p^k (1-p)^k$
    - Geometric: $P(X=k) = p(1-p)^{k-1}$
    - Poisson: $\frac{\lambda^n t^n}{n!} e^{-\lambda t}$
  - $E(X) = \sum x_i p_i$
    - Binomial: np
    - Geometric: $1/p$
    - Poisson: λt

- Elementary group theory.
- RSA

  take p, q. $n = pq$. $\phi(n) = (p-1)(q-1)$

  select e, d st $ed = 1 \mod \phi(n)$

  pubkey = (e, n)

  Encrypt: $c = m^e \mod n$

  Decrypt: $m = c^d \mod n$

- El gamal:

  Take $\mathbb{Z}_p^*$, g, random x

  $h = g^x \mod p$

  pubkey = $(h, p, \ )$

  Encrypt: Take random y

  $s = h^y \mod p$

  $$\boxed{\begin{aligned} c_1 &= g^y \mod p \\ c_2 &= ms \mod p \end{aligned}}$$

  Decrypt

  $$\boxed{m = (c_1^x)^{-1} c_2 \mod p}$$

Integer Factorization:

In $ed = 1 \mod n$

given e, n

d is hard to get.

Discrete Log:

In $g^x = h \mod p$

given h, g, p

x is hard to get.

- Cryptographic Puzzle
  - Find nonce s.t.

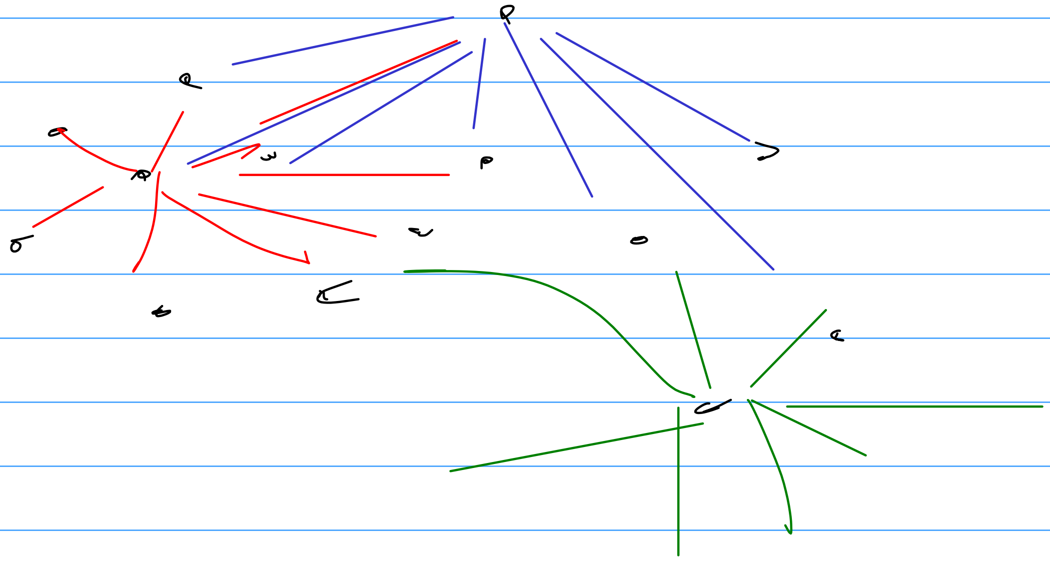
    $H(\text{nonce} \,||\, \text{sig} \,||\, \text{tx} \ldots) < \text{target}$.
  - If $\text{target} = 2^{256-k}$

    $E(\text{trials}) = 2^k$
- Limit on coins $= 50\left(1 + \frac{1}{2} + \frac{1}{4} + \cdots\right) K$

Block Structure

no.	Txn Hash	Fee	Amt	Sender	Receiver
0	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
1					
2					
3					

Gossip protocol. TCP 8333



- Hot and Cold Storage

Cold Side: seed, x, y, i^{th}

i, pr: $x_i = x + H(\text{seed} \mid i)$

i, pub: $g^{x_i} = g^{x} \cdot g^{H(\text{seed} \mid i)}$ $\quad g^x = y$

Hot Side: seed, g^y

i, pub $= g^{x_i} = y \cdot g^{H(\text{seed} \mid x)}$

i, addr $= H(g^{x_i})$

- Brain Wallets

  - Entropy $= -\sum_{k=1} p_k \log(p_k)$

- Currency Exchange Rate:

Total supply of BTC $\leftarrow$ $\dfrac{S}{D} = \dfrac{T}{P}$ $\rightarrow$ Total transaction value US

Duration of circulation $\leftarrow$ D $\quad$ P $\rightarrow$ Price of BTC.

- Stealth Address:

publish: g, y st $y = g^x \bmod p$.

Pay: pubkey $= H(y^r)$

prkey $= xr$

- Attacks:
  - Linking Attacks
  - Change Address Attacks
  - Network Layer Attack
  - taint Analysis.

- ZKP
  - Examples TODO $c = g^r \bmod p$

- Satoshi's Paper

Gambler's deficit.

p = positive, q = negative, q_r = takeover.

$$q_r = \begin{cases} 1 & \text{if } p < q \\ \left(\frac{q}{p}\right)^n & \text{if } p \geq q \end{cases}$$

blocks mined after

Attacker's progress: $\lambda = z\dfrac{q}{p}$

(Poisson distr)

$$P = \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{z-k} & k \leq z \\ 1 & k > z \end{cases}$$

or $$P = 1 - \sum_{n=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - \left(\frac{q}{p}\right)^{z-k}\right)$$

- Epsilon-Differentially Private

$$Pr(M(x) \in E) \le e^{\epsilon} Pr(M(y) \in E) \quad \forall E \subset S$$

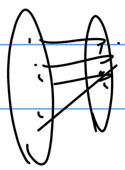
- Privacy Loss ϵ

↳

or $$\ln \frac{Pr(M(x) \in E)}{Pr(M(y) \in E)} \quad \forall E \subset S.$$

- ϵ-differentially private maps over functions

$$Pr(f \circ M(x) \in E) \le e^{\epsilon} Pr(M(y) \in E)$$



$$E_2 = \{x \in S \mid f(x) \in E_1\}$$

$$\boxed{Pr(f \circ M(x) \in E_1) = Pr(M(x) \in E_2)}$$

$$\Rightarrow Pr(f \circ M(x) \in E_1) \le e^{\epsilon} Pr(f \circ M(y) \in E_2)$$

$$\Rightarrow Pr(f \circ M(x) \in E_1) \le e^{\epsilon} Pr(f \circ M(y) \in E_1)$$

- Laplace noise

Probability ϵ-diff.

✓ $$f(x \mid \mu, b) = \frac{1}{2b} e^{\left(-\frac{|x-\mu|}{b}\right)} \qquad Lap\left(\frac{1}{\epsilon n}\right)$$

- Loss: $$\ln\left(\frac{Pr(M(x) = z \mid x = (n-k, k))}{Pr(M(y) = z \mid z = (n-k+1, k))}\right)$$

noise = $z - \mu_x$

$$\ln\left(\frac{\frac{\epsilon n}{2} e^{-|z-\mu_x|\epsilon n}}{\frac{\epsilon n}{2} e^{-|z-\mu_y|\epsilon n}}\right) = \ln e^{\epsilon n(|z-\mu_y| - |z-\mu_x|)}$$

$$<= \ln e^{\epsilon n |\mu_x - \mu_y|}$$

$$\le \epsilon n \underbrace{|\mu_x - \mu_y|}_{\text{to } \frac{1}{n}}$$

$$\le \epsilon$$

Keep in mind :

- Differential Privacy :

- $P(M(x) \in E) \leq e^{\epsilon} \Pr(M(y) \in E) \; \forall E \subseteq S$

- Privacy loss $= \ln\left(\dfrac{\Pr(M(x) \in E)}{\Pr(M(y) \in E)}\right)$

- Risk $= E(\text{noise})^2$