An Aggie does not lie, cheat or steal or tolerate those who do. $\mathbb{P}$ is the set of primes. $\mathbb{P}^{odd}$ is the set of odd primes.
$a \mid b \wedge b \mid c \to a \mid c$. $a \mid b \wedge b \mid a \to a = \pm b$.
$a \mid b \wedge a \mid c \to \forall u, v \in \mathbb{Z}, a \mid (ub + vc)$
Extended Euclidean Algorithm: $\exists u, v \in \mathbb{Z}, au + bv = \gcd(a, b)$
$\exists u, v \in \mathbb{Z}, au + bv = c \to \gcd(a, b) \mid c$
Fermat's Little Theorem: $p \in \mathbb{P} \to \forall a \in (\mathbb{Z}/p\mathbb{Z})^*, a^{p-1} \equiv 1 \mod p$
n is a composite number and $b^n \equiv b \mod n, \forall b \in \mathbb{Z} \to n$ is a **Carmichael number**.
Order: The smallest $k \in \mathbb{Z}^+$ such that $g^k \equiv 1 \mod p$
Primitive Root: $g \in (\mathbb{Z}/p\mathbb{Z})^*, \text{order}(g) = p - 1 \to g$ is a primitive root.
Inverse of $a \mod p \leftrightarrow \exists b \in \mathbb{Z}, a \cdot b \equiv 1 \mod p$. $a \nmid p$
Let $m \in \mathbb{Z}^{odd}$. $\dfrac{(b-1)m+1}{b} \equiv b^{-1} \mod m$
Euler's Totient Function: $\phi(n)$ = the number of invertible elements in $\mathbb{Z}/n\mathbb{Z}$
Primitive Root Theorem: There are exactly $\phi(p-1)$ primitive roots mod p
$p \in \mathbb{P} : q^{\frac{p-1}{2}} \in \mathbb{P}, g \in (\mathbb{Z}/p\mathbb{Z})^*$. order $(g) = \{1, 2, q, 2q\}$.
$p \in \mathbb{P}, g$ proot, $a \in \mathbb{Z} \to$ order $(g^a) = \dfrac{p-1}{\gcd(a, p-1)}$
Discrete log: Given $p \in \mathbb{P}$, primitive root g, target value y. Calculate x such that $g^x \equiv y \mod p$
We assume that there is no efficient algorithm to solve DLP or DHP.
Diffie-Hellman Problem. Given $p \in \mathbb{P}$, primitive root g. $A = g^a \mod p, B = g^b \mod p$ compute $g^{ab} \mod p$, $DHP \leq_p DLP$
ElGamal. Encrypt: $(c_1, c_2) = (g^k, mB^k)$, Decrypt: $m \equiv (c_1^k)^{-1} c_2 \mod p$, $DHP \leq_p ElGamal \leq_p DLP$. Insecure against Chosen Ciphertext attack.
RSA. $N = pq, p, q \in \mathbb{P}, e \in \mathbb{Z}, \gcd(e, \phi(N)) = 1, ed \equiv 1 \mod \phi(N)$. Encrypt: $C = m^e \mod N$. Decrypt: $m \equiv C^d \mod N$
$RSA \leq_p Factoring$. We assume we cannot efficiently factor integers.
Due to Pollard's $p-1$ algorithm, if $p-1$ is B-smooth for small B, RSA can be efficiently decrypted.
If N can be factored, signature can be forged. Signature can be efficiently forged on some document, unknown for any document.
A square root of a modulo p is an integer x such that $x^2 \equiv a \pmod p$. Computing square roots mod N of arbitrary quadratic residues N is of same difficulty as factoring.
For $N = pq$, there are $0, 2, 4$ square roots of $a \mod N$. If $N|a$, there are 0. If $\gcd(a, N) = p \vee q$, there are 2. If $\gcd(a, N) = 1$, there are 4.
For $N = pq$ where $p, q \in \mathbb{P}^{odd}$ are distinct, if $\exists a, b \in \mathbb{Z}, a^2 \equiv b^2 \pmod N \wedge a \not\equiv \pm b \pmod N$, then $\gcd(a \pm b, N)$ is a nontrivial factor of N.
Chinese Remainder Theorem: Let $m_1, \cdots, m_k$ be pairwise co-prime integers. $\forall a_1 \cdot a_k \in \mathbb{Z}$ the system of congruences
$x \equiv a_1 \mod m_1, x \equiv a_2 \mod m_2, \cdots, x \equiv a_k \mod m_k$ has a unique solution $\mod m_1 m_2 \cdots m_k$
$\exists x, x^2 \equiv b \mod p \to \forall e \geq 1, \exists x, x^2 \equiv b \mod p^e$
$\gcd(a_1, a_2, \cdots, a_k) = 1 \to \exists u_1, u_2, \cdots, u_k \in \mathbb{Z}, a_1 u_1 + a_2 u_2 + \cdots + a_k u_k = 1$
Fermat–Euler theorem: Let $N = pq, p, q \in \mathbb{P}$. Let $a \in \mathbb{Z}$.
$\gcd(a, N) = 1 \to a^{\phi(N)} \equiv 1 \mod N$
A **group** is a set G together with a binary operation $* : G * G \in G$ satisfying the following three properties:
Identity Law: $\exists e \in G, \forall g \in G, e * g = g * e = g$.
Inverse Law: $\forall g \in G, \exists h \in G, g * h = e = h * g$.
Associative Law: $\forall g, h, k \in G, (g * h) * k = g * (h * k)$
An **abelian** group satisfies the **Commutative Law**: $\forall g, h \in G, g * h = h * g$
Let $\mathcal{G} = (G, *)$ is a finite group $\to \forall g \in G, \text{order}(g)$ is finite.
Let $g \in \mathcal{G}$, order $(g) = d \wedge g^k = e \to d \mid k$
Lagrange's Theorem: Let $\mathcal{G} = (G, *)$ be a finite group. Let $g \in \mathcal{G}$. order $(g) \mid |G|$.
$\forall g \in (G, *), N = \text{order}(g), d \mid N, \text{order}(g^d) = \dfrac{N}{d}$.
$\exists x, ax \equiv c \mod m \leftrightarrow \gcd(a, m) | c$.

n is a composite number $\leftrightarrow n$ has a **Miller-Rabin** witness.
Let $p \in \mathbb{P}$. Let $a \in (\mathbb{Z}/p\mathbb{Z})^*$. $x, y \in \mathbb{Z}, x = y \mod p - 1 \to a^x \equiv a^y \mod p$
$n \in \mathbb{Z}$ is ***B*-smooth** $\leftrightarrow$ every prime factor of n is at most B.
Let $N \in \mathbb{Z}^+$. Let f denote the polynomial $f(x) = x^2 - N$. Let $p \in \mathbb{P}^{odd}$. Let $a \in \mathbb{Z}$. $a^2 \equiv N \mod p \leftrightarrow p \mid f(a)$
Let $m \in \mathbb{Z}$. a is a **quadratic residue** $\leftrightarrow \exists c \in \mathbb{Z}, c^2 \equiv a \mod m$
Let $p \in \mathbb{P}^{odd}$, g is proot, $a \equiv g^k \mod p$.
a is a QR $\mod p \leftrightarrow k \mid 2$
If $p \in \mathbb{P}, p \equiv 3 \mod 4$, and a is a QR, $a^{\frac{p-1}{4}}$ is a sqroot of $a \mod p$.
$p \in \mathbb{P}^{odd}$, there exists exactly 2 integers $x \in \mathbb{Z}/p\mathbb{Z}$ such that $x^2 \equiv 1 \mod p$.
p is an odd prime power, there are exactly 2 square roots of $1 \mod p$.
The number of square roots of $1 \mod 2^k = \begin{cases} 1 & \text{if } k = 1 \\ 2 & \text{if } k = 2 \\ 4 & \text{if } k \geq 3 \end{cases}$
Legendre Symbol: Let $p \in \mathbb{P}^{odd}$, $\left(\dfrac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a QR } \mod p \\ -1 & \text{if } a \text{ is a NQR } \mod p \\ 0 & \text{if } a \equiv 0 \mod p \end{cases}$
Euler's Criterion: $a^{\frac{p-1}{2}} \equiv \left(\dfrac{a}{p}\right) \mod p$
$p \in \mathbb{P}^{odd}, a^{\frac{p-1}{2}} \equiv \begin{cases} 1 & \text{if } a \text{ is a QR} \\ -1 & \text{if } a \text{ is a NQR} \end{cases}$.
Gauss Theorem: Let $a, b \in \mathbb{Z}^{odd}$. $\left(\dfrac{-1}{b}\right) = \begin{cases} 1 & \text{if } b \equiv 1 \mod 4 \\ -1 & \text{if } b \equiv 3 \mod 4 \end{cases}$
$\left(\dfrac{2}{b}\right) = \begin{cases} 1 & \text{if } b \equiv \pm 1 \mod 8 \\ -1 & \text{if } b \equiv \pm 3 \mod 8 \end{cases}$
$\left(\dfrac{a}{b}\right) = \begin{cases} \left(\dfrac{b}{a}\right) & \text{if } a \equiv 1 \mod 4 \vee b \equiv 1 \mod 4 \\ \left(-\dfrac{b}{a}\right) & \text{if } a \equiv 3 \mod 4 \wedge b \equiv 3 \mod 4 \end{cases}$
$\left(\dfrac{a}{b}\right) = 1 \not\to a$ is a qr. $\left(\dfrac{a}{b}\right) = -1 \to a$ is a nqr.
Honest Verifier Zero Knowledge: $\exists$ an efficient algorithm that can produce transcripts that are indistinguishable from the transcripts of the an honest interaction.
Completeness: If the statement is true, an honest verifier will be convinced of this fact by an honest prover.
Soundness: If the statement is false, no cheating prover can convince an honest verifier that it is true, except with some small probability. Cannot produce 2 unique transcripts without knowing the key.
Zero Knowledge: If the statement is true, no verifier learns anything other than the fact that the statement is true. To prove, apply the protocol in reverse.
Elliptic Curve: $E : y^2 = x^3 + ax + b, 4a^3 + 27b^2 \neq 0$
$m = \begin{cases} \dfrac{y_Q - y_P}{x_Q - x_P} & \text{if } x_P \neq x_Q \\ \dfrac{3x_P^2 + a}{2y_P} & \text{if } P = Q \end{cases}$
$x_{P+Q} = m^2 - x_P - x_Q, y_{P+Q} = m(x_P - x_{P+Q}) - y_P$
Hasse bound: Every Elliptic Curve over $\mathbb{F}_p$ has a size $[p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$.
Average size $p + 1$ because half are QR, max size $2p + 1$.
Size of E calculation in $\mathcal{O}(\log^6 p)$ by Schoof, $\mathcal{O}(\log^4 p)$ with SEA.
Order of Point P is smallest k such that $P \cdot k = \mathcal{O}$, $\mathcal{O}$ is point at infinity.
Birthday Paradox: Assume a uniformly random distribution of birthdays. You need 23 people to have a likely chance on two of them share a birthday. However you need 253 people to have a likely chance that one of them shares your birthday.
E3Q7 Proof:
$p \in \mathbb{P}, p = 2q + 1$. Prove that there exists as element of $(\mathbb{Z}/p\mathbb{Z})^*$ with order q.
See Primitive Root Theorem.

EC DLP: Given $p \in \mathbb{P}^{odd}, E \in \mathbb{F}_p$, base point $P \in E$, target point $Q \in E$. Calculate n such that $Q \equiv nP \mod p$. Fastest known solution $O(\sqrt{p})$.
EC DHP: Given $p, E \in \mathbb{F}_p, P \in E, Q_A = n_A P, Q_B = n_B P$. Compute $n_A n_B P \mod p$. EC DHP $\leq_p$ EC DLP
EC ElGamal: Public: $p \in \mathbb{P}, E, \mathbb{F}_p, P \in E$. $Q_A = n_A P$.
Encrypt: $(c_1, c_2) = (kP, m + kQ_A)$. Decrypt: $m = c_2 - n_A c_1$. m encoded as point on P.
Pohlig-Hellman Algorithm:
Calculates Discrete Log, can be efficient for DLP of small order.
Collision Algorithm $\mathcal{O}(n \log n) \approx \mathcal{O}(2^{\frac{k}{6}} \cdot k)$
Input: $\mathcal{G} = (G, *)$ finite group, $g \in \mathcal{G}, h \in \mathcal{G}$, order $(g) = d$

1. $n = \left\lfloor \sqrt{d} \right\rfloor + 1$
2. $L_1 = \left\{g^0, g^1, \cdots, g^n\right\}, L_2 = \left\{hg^{-0}, hg^{-n}, \cdots, hg^{-n^2}\right\}$
3. Find $0 \leq i, j < n$ such that $g^i = hg^{-jn}$
4. Return $i + jn$

EC DLP Collision Algorithm $\mathcal{O}(\sqrt{p})$

1. $L_1 = \{y_1 P, y_2 P, \dots y_r P\}, L_2 = \{z_1 P + Q, z_2 P + Q, \dots z_r P + Q\}$
2. Find collision $y_i P = z_j P + Q$
3. $Q = (y_i - z_i) P$

If $r \approx 3\sqrt{\text{order} P} \leq 3\sqrt{P}$, collision odds $\geq 99\%$.
Pollard's ρ algorithm
Input: $x_0 \in S, y_0 \in S, n \in \mathbb{Z}, f: S \to S$

1. $d = 0$
2. Repeat until $1 < d < n$
3. $x_i = f(x_{i-1}), y_i = f(f(y_{i-1}))$
4. $d = \gcd(x - y, n)$

Schnorr Digital Signature Algorithm
Apply Fiat-Shamir Transform to ZKP
$p \in \mathbb{Z}, p = kq + 1$ for some small k, g, order $(g) = q$
Secret key $a \in \mathbb{Z}/q\mathbb{Z}$. Public key $A \equiv g^a \mod p$. $H(C, D)$ random oracle.
Sign:

1. "commitment": Pick random $c \in \mathbb{Z}/q\mathbb{Z}$, compute $C \equiv g^c \mod p$
2. "challenge": $h = H(C, D)$
3. "response": $r = c + ah$
4. "signature": $S = (C, r)$

Verify: $g^r \equiv C \cdot A^h \mod p$
EC Schnorr DSA:
$p \in \mathbb{P}, E \in \mathbb{F}_p, P \in E$
Secret key $n_A \in \mathbb{Z}/q\mathbb{Z}$. Public key $Q_A \equiv n_A P \mod p$. $H(C, D)$ random oracle.
Sign:

1. "commitment": Pick random $c \in \mathbb{Z}/q\mathbb{Z}$, compute $C \equiv cP \mod p$
2. "challenge": $h = H(C, D)$
3. "response": $r = c + n_A h$
4. "signature": $S = (C, r)$

Verify: $rP \equiv C + hQ_A$

Lenstra's EC Factoring Algorithm Find k such that $k! \cdot P \equiv \mathcal{O} \mod p$ and $k! \cdot Q \not\equiv \mathcal{O} \mod p$
Similar to Pollard's $p - 1$ algorithm, but for EC.
Input: $p \in \mathbb{P}, E \in \mathbb{F}_p, P \in E$

1. $j = 2$
2. Repeat until slope calculation failure
3. $P = jP$
4. $j = j + 1$

When calculating the inverse of the difference of x coordinates in calculating the slope.
$\gcd(\Delta x, N)$ is the factor.
Dual EC Deterministic Random Bit Generator
Public fields: $p \in \mathbb{P}, E \in \mathbb{F}_p, P, Q \in E$.
Initial seed = s_0. Future seeds calculated as $S = \{x(s_0 P), x(s_1 P), \dots\}$
Random numbers generated as $R = \{x(s_1 Q), x(s_2 Q), \dots\}$, with 16 most significant bits discarded.
Is innately a bad PRNG, attacker can predict bits with 50.11 accuracy.
Dual EC DRBG "Backdoor"
If n of $Q = nP$ is known, can predict all future outputs.
Known to hacker: $n, r_i = x(s_i Q)$
Brute force / guess 16 bits, $2^{16} = 65536$ possibilities to get point $s_i(Q)$.
Compute $n \cdot (s_i Q) = s_i \cdot (nQ) = s_i P = s_{i+1}$
Can be closed by discarding more bits, or showing how Q was chosen.

ZKP and DSA: $p \in \mathbb{P}, p = 2q + 1, q \in \mathbb{P}, g \in (\mathbb{Z}/p\mathbb{Z})^*$ has order q. Let $\langle g \rangle = \{1, g, g^2, \dots, g^{q-1} \mod p\}$. Let $A \in \langle g \rangle$ such that $g^a \equiv A \pmod p$ for secret key a,

- Peggy sends random commitment $C \in \langle g \rangle$
- Victor sends random challenge $h \in \mathbb{Z}/q\mathbb{Z}$
- Peggy sends response $r \in \mathbb{Z}/q\mathbb{Z}$
- Victor accepts if $g^r \equiv C \cdot A^h \mod p$

Produce indistinguishable transcripts (**ZK**):
Choose random $h \in \mathbb{Z}/q\mathbb{Z}$
Choose random $c \in \mathbb{Z}/q\mathbb{Z}$
Define $C = g^c \cdot A^{-h}, r = c$
Transcript = (C, h, r)
Soundness: given $(C, h_1, r_1), (C, h_2, r_2), h_1 \not\equiv h_2 \mod p$
$C \equiv g^{r_1} A^{h_1} \equiv g^{r_2} A^{h_2}$
$a = (r_2 - r_1) \cdot (h_2 - h_1)^{-1} \mod q$
Turn this into **Signature**:
Secret key a. $C = g^c$
$h = H(C, D) \mod q$, H is random oracle
$r = c + ah \mod q$
Send $S = (C_0, C_1, \cdots, C_i, r_0, r_1, \cdots, r_i)$
Victor generates C and Peggy responds with r until Victor is "convinced" that Peggy knows the secret key.
Tonelli-Shanks Algorithm (calculate sqroot in $O(\sqrt{n})$):
Let $p \in \mathbb{P}^{odd}, p - 1 = 2^k Q, Q \equiv 1 \mod 2$, z is a NQR

1. If $a^Q \equiv 1 \mod p$, return $a^{\frac{Q+1}{2}} \mod p$
2. for $i \in [0, k - 1)$:
3. If $a^{2^i Q} \equiv -1 \mod p$
   (a) $a' = az^{2^{k-i-1}} \mod p$
   (b) $R = \sqrt{a'}$
   (c) return $Rz^{-2^{k-i-2}} \mod p$
4. Else $i = i + 1$