Introductie: vertel onderwerp van de scriptie.

- Let doel van cryptografie uit:
  - geheimhouding: Alice stuurt bericht naar Bob en Eve kan het niet begrijpen.
  - authentifisering: Alice stuurt bericht naar Bob zdd Bob zeker weet dat het bericht echt door Alice gestuurd is.
  - integriteit: Alice stuurt bericht naar Bob en Bob weet zeker dat het bericht onderweg niet veranderd is.
- Leg verschil uit tussen symmetrische en asymmetrische (public key) cryptografie.
- Leg uit dat cryptografie gebasseerd is op problemen die 'makkelijk' te creëren en 'moeilijk' op te lossen zijn.
- Leg termen polynomial time, subexponential time en exponential time uit.
- Voorbeeld: DLP en priemfactorizatie. Merk op, DLP oplossing uniek modulo $N = \text{ord}(P)$.
- RSA-methode: p, q priemgetallen, $N = pq$, dan $G = (\mathbb{Z}/N\mathbb{Z}^*, \cdot)$. Merk op dat het probleem is een inverse van $e \in G$ berekenen.
  - Als p en q bekend zijn, dan kan e^{-1} berekent worden door uitgebreide euclidische algorithme, i.e., bereken $\gcd(e, (p-1)(q-1) = \#G)$.
  - Los $e^k = 1$ op voor k. Is DLP. dan $e^{-1} = e^{k-1}$.
- Andere groepen, gebruikt voor DLP. (Makkelijk te definieren, elementaire operaties zijn efficient te berekenen en DLP is relatief moeilijk op te lossen.)
  - $q = p^n$ voor p een priemgetal, dan $G = (\mathbb{F}_q^*, \cdot)$. DLP kan relatief snel opgelost worden met behulp van index calculus method.
  - Elliptische kromme over een eindig lichaam, groepen waarvoor DLP exponentieel in het algemeen is.
- Leg notatie voor affine en projectieve coordinaten $\mathbb{A}^2(\mathbb{F}_q)$ en $\mathbb{P}^2(\mathbb{F}_q)$ uit.
- Kies priemmacht $q = p^n$, eindig lichaam $\mathbb{F}_q$. Dan is een elliptische kromme gegeven door

$$E := \{[X, Y, Z] \in \mathbb{P}^2(\mathbb{F}_q) \mid Y^2Z = X^3 + AXZ^2 + BZ^3\}.$$

- $Z \neq 0$, dan gebruik affine coordinaten $x := X/Z$ en $y := Y/Z$.
- E kan gegeven worden in affine coordinaten x, y door

$$E := \{(x, y) \in \mathbb{A}^2(\mathbb{F}_q) \mid y^2 = x^3 + Ax + B\}$$

  samen met een uniek punt $O = [0, 1, 0]$ in oneindig.
- Let groupsstructuur van E uit. O is eenheids element van deze structuur.
- $P \in E$, $m \in \mathbb{Z}$, dan leg uit wat $[m]P$ is.
- $P \in E$ orde N en $Q \in \langle P \rangle$, dan $[m]P = Q$ oplossen voor $m \in \mathbb{Z}/N\mathbb{Z}$ is ECDLP.
- ECDLP is niet altijd 'moeilijk' om op te lossen. In mijn scriptie bekijk ik meerdere aanvallen op dit probleem:

- Algemene aanvallen.
  * Deze bepalen hoe groot de orde van P minimaal moet zijn. Dus geeft ook een idee van hoe groot $\#E$ moet zijn. (Let uit hoe $\#E$ afhangt van q, i.e., geef Hasse's stelling.)
  * Pohlig Hellman methode. Bepaald dat orde van P een groot priemgetal moet zijn.
- Aanvallen op specifieke krommen. Deze bepalen welke eigenschappen de kromme E en het punt P moet hebben om te zorgen dat de ECDLP 'moeilijk' is.

- Als er nog meer tijd over is, kan ik uitleggen wat de 'trace of Frobenius' t is, dat er een algoritme (Schoof's algorithme) bestaat die $\#E$ berekent, en dat er aanvallen op krommen E zijn voor $t = 0, 1, 2$.