# Voorblad

**Titel: cryptografie in het huidige tijdperk**

**Hoofdvraag: Op welke manier kan cryptografie worden toegepast om de veiligheid en privacy van digitale communicatie te waarborgen binnen een evoluerende technologische omgeving?**

# Samenvatting

## Inleiding

Dit onderzoek verkent de functie van cryptografie in het beschermen van de veiligheid en privacy van digitale communicatie. De hoofd vraag die het onderzoek probeert te beantwoorden is: “Op welke manier kan cryptografie worden toegepast om de veiligheid en privacy van digitale communicatie te waarborgen binnen een evoluerende technologische omgeving?”

## Doelstelling

Het doel van dit onderzoek is om een duidelijk inzicht te krijgen in de basisprincipes van cryptografie, de ethische en maatschappelijke gevolgen ervan, en de huidige en opkomende bedreigingen waar het veld van cryptografie momenteel tegenaan loopt.

## Bevindingen

De bevindingen van het onderzoek illustreren de fundamentele concepten van cryptografie, vertrouwelijkheid, integriteit en authenticatie. Het onderzoek benadrukt ook de dubbelzijdige aard van cryptografie, waarbij het privacy en veiligheid beschermt maar ook mogelijk misbruik door criminelen en ethische dillema’s met zich meebrengt. Er wordt ook gekeken naar de problemen en risico’s van cryptografie met betrekking tot nieuwe technologieën, zoals kwantumcomputers.

## Conclusies

De belangrijkste conclusies van het onderzoek suggereren dat cryptografie effectief kan worden toegepast en voortdurend kan worden verbeterd door een grondig begrip van de basisprincipes, een bewuste afweging van de ethische en maatschappelijke gevolgen, en een proactieve aanpak van kritieke en opkomende bedreigingen. Het onderzoek benadrukt de noodzaak van voortdurende innovatie om de veiligheid van gegevens te waarborgen in de steeds veranderende technologische omgeving. Het onderzoek concludeert ook dat toekomstig onderzoek zich zou moeten richten op het aanpakken van de uitdagingen en bedreigen waar cryptografie mee te maken heeft, zoals kwantumcomputers. En het onderzoeken van mogelijke oplossingen voor de ethische dillema’s die cryptografie met zich meebrengt

# Inhoudsopgave

Table of Contents

[Voorblad 1](#_Toc167880573)

[Samenvatting 2](#_Toc167880574)

[Inleiding 2](#_Toc167880575)

[Doelstelling 2](#_Toc167880576)

[Bevindingen 2](#_Toc167880577)

[Conclusies 2](#_Toc167880578)

[Inhoudsopgave 3](#_Toc167880579)

[Inleiding 5](#_Toc167880580)

[Aanleiding van het onderzoek 5](#_Toc167880581)

[Doelstelling 5](#_Toc167880582)

[Hoofd- en deelvragen 5](#_Toc167880583)

[Hoofdvraag 5](#_Toc167880584)

[Deelvragen 5](#_Toc167880585)

[Aanpak 5](#_Toc167880586)

[Structuur 6](#_Toc167880587)

[Basisprincipes van cryptografie 7](#_Toc167880588)

[Uit welke principes bestaat cryptografie? 7](#_Toc167880589)

[Vertrouwelijkheid 7](#_Toc167880590)

[Integriteit 7](#_Toc167880591)

[Authenticatie 7](#_Toc167880592)

[Waarom vormen deze principes de basis van cryptografie? 7](#_Toc167880593)

[Conclusie 8](#_Toc167880594)

[Huidige en opkomende bedreigingen 8](#_Toc167880595)

[Sleutelbeheer 8](#_Toc167880596)

[Kwetsbaarheden in algoritmen 8](#_Toc167880597)

[Kwantumcomputers 8](#_Toc167880598)

[Conclusie 8](#_Toc167880599)

[Ethische en maatschappelijke implicaties 9](#_Toc167880600)

[Waarborgen van privacy 9](#_Toc167880601)

[Verkrijgen van toegang tot versleutelde communicatie 9](#_Toc167880602)

[Evenwicht tussen veiligheid en privacy 9](#_Toc167880603)

[Conclusie 9](#_Toc167880604)

[Conclusie 10](#_Toc167880605)

[Literatuurlijst 11](#_Toc167880606)

# Inleiding

## Aanleiding van het onderzoek

In een tijdperk waarin digitale communicatie de norm is geworden, is het belangerijk om de veiligheid van deze communicatie te waarborgen. Cryptografie speelt een belangerijke rol bij het beveiligen van gegevens en het beschermen van privacy. Echter, met de constante vooruitgang van technologieën en de opkomst van nieuwe bedreigingen, ontstaan er steeds nieuwe uitdagingen en vraagstukken.

## Doelstelling

Dit onderzoek hoopt een inzicht te bieden in de huidige stand van zaken omtrent cryptografie, met specifieke aandacht voor de uitdagingen, toepassingen en toekomstige ontwikkelingen. Door verschillende aspecten van cryptografie te verkennen, hopen we een beter begrip te krijgen van hoe deze discipline kan bijdragen aan het waarborgen van digitale veiligheid en privacy.

## Hoofd- en deelvragen

### Hoofdvraag

“Op welke manier kan cryptografie worden toegepast om de veiligheid en privacy van digitale communicatie te waarborgen binnen een evoluerende technologische omgeving?”

### Deelvragen

1. Wat zijn de basisprincipes van cryptografie?
2. Wat zijn de ethische en maatschappelijke implicaties van het gebruik van cryptografie, met specifieke aandacht voor privacy, surveillance en vrijheid van meningsuiting?
3. Welke actuele uitdagingen en bedreigingen zijn er binnen cryptografie?

## Aanpak

Het onderzoek zal zich concentreren op een analyse van bestaande literatuur en bronnen over cryptografie. Relevante literatuur zal worden onderzocht om inzicht te krijgen in de principes, methoden, uitdagingen en toepassingen van cryptografie. Door deze bronnen te bestuderen en te analyseren, hopen we naar een mooi begrip van het onderwerp en naar het beantwoorden van de hoofd- en deelvragen.

## Structuur

1. **Voorblad**: Het voorblad bevat de titel van het onderzoek, informatie over de student en de hoofdvraag.
2. **Samenvatting**: Dit is een samenvatting van het onderzoek, met een inleiding op het onderwerp, de hoofdvraag, het doel van het onderzoek, bevindingen, en de conclusies.
3. **Inhoudsopgave**: Dit geeft een overzicht van de inhoud van het onderzoek.
4. **Inleiding**: Dit deel bevat de aanleiding van het onderzoek, de doelstelling, de hoofd- en deelvragen, de aanpak, en de structuur van het onderzoek.
5. **Hoofdstukken**: Elk hoofdstuk beantwoord een deelvraag. Het bevat een korte alinea, een bevindingen uit de bronnen, en een afsluitende alinea met een conclussie gebasseerd op de belangrijkste bevindingen en een antwoord op de deelvraag.
6. **Conclusie**: Dit deel herhaald de hoofdvraag, vat de deelconclusies samen, analyseert deze om patronen te vinden, geeft een beargumenteerd antwoord op de hoofdvraag op basis van de analyse van de deelconclusies, en geeft suggesties voor een mogelijk toekomstig onderzoek.
7. **Literatuurlijst**: Dit is een lijst van literatuur die is gebruikt in het onderzoek, deze zijn opgemaakt in APA stijl.

# Basisprincipes van cryptografie

Cryptografie, afkomstig van de Oudgriekse woorden ‘kruptós’, wat ‘verborgen’ betekent, en ‘gráphein’, wat ‘schrijven’ betekent, is de wetenschap die, zoals de naam al suggereert, draait om het verbergen van informatie. In het huidige technologische landschap speelt cryptografie een cruciale rol bij het beschermen van informatie.

### Uit welke principes bestaat cryptografie?

De drie fundamentele basisprincipes van cryptografie zijn:

1. **Vertrouwelijkheid**: Dit principe zorgt ervoor dat de informatie alleen toegankelijk is voor degenen die daarvoor geautoriseerd zijn.
2. **Integriteit**: Dit principe zorgt ervoor dat de informatie niet kan worden gewijzigd op een ongeautoriseerde manier.
3. **Authenticatie**: Dit principe verifieert de identiteit van de partijen die betrokken zijn bij de communicatie.

Deze principes vormen de basis van cryptografie [1] en zijn essentieel voor het waarborgen van de veiligheid en privacy van digitale communicatie.

### Vertrouwelijkheid

Vertrouwelijkheid waarborgt dat de informatie enkel toegankelijk is voor degenen die de juiste autorisatie hebben [2]. Dit wordt gerealiseerd door het toepassen van encryptie, die de gegevens versleuteld zodat ze niet bruikbaar zijn zonder de correcte sleutel.

### Integriteit

Integriteit waarborgt dat tijdens de overbrenging de gegevens ongewijzigd blijven. Dit wordt voornamelijk bereikt door het toepassen van hash-functies en digitale handtekeningen. Hash-functies vormen een unieke hash-waarde van de gegevens, die wijzigt als de gegevens worden aangepast. Digitale handtekeningen gebruiken deze hash-waarden om te controleren dat de gegevens niet zijn gewijzigd sinds ze werden ondertekend.

### Authenticatie

Authenticatie is cruciaal voor veilige communicatie. Het verifieert de identiteit van de communicerende partijen, en voorkomt ongeautoriseerde toegang. Authenticatie kan bijvoorbeeld worden bereikt met wachtwoorden of digitale certificaten. Het beschermt gevoelige gegevens en bevestigt identiteiten voordat gegevensuitwisseling plaatsvindt. Hoewel het de identiteit verifieert, garandeert het niet de integriteit en vertrouwelijkheid van de overgedragen gegevens. Daarvoor zijn extra beveiligingsmaatregelen zoals encryptie en digitale handtekeningen nodig.

### Waarom vormen deze principes de basis van cryptografie?

De drie fundamentele principes van cryptografie - vertrouwelijkheid, integriteit en authenticatie - zijn van belang omdat ze de uitdagingen aangaan die gepaard gaan met het beveiligen van digitale informatie. In een digitale wereld waarin informatie kan worden gekopieerd, aangepast en verspreid, bieden deze principes de instrumenten om de veiligheid van onze communicatie en gegevens te waarborgen.

## Conclusie

Het begrijpen en toepassen van de fundamentele principes van cryptografie - vertrouwelijkheid, integriteit en authenticatie - is belangrijk voor het waarborgen van veilige communicatie in een digitale omgeving. Deze principes stellen ons in staat om systemen te creëren die bestand zijn tegen diverse soorten aanvallen en die de veiligheid en privacy van gebruikers garanderen.

# Huidige en opkomende bedreigingen

Cryptografie, speelt een belangrijke rol in onze samenleving. Echter, zoals bij elke technologie, zijn er bedreigingen en uitdagingen. In deze paragraaf zullen we ons richten op: kwetsbaarheden in cryptografische algoritmen, de uitdagingen van sleutelbeheer en de opkomst van kwantumcomputers.

## Sleutelbeheer

Het veilig opslaan van privésleutels is belangrijk, maar helaas gaat het hier vaak mis [3]. Het komt regelmatig voor dat de geheime sleutels van grote bedrijven worden gestolen. Het grootste probleem is dat bedrijven dit vaak pas te laat ontdekken. De personen die de geheime sleutel hebben bemachtigd, kunnen deze misbruiken om virussen en andere schadelijke software als legitiem te laten lijken. Het is dus van belang dat bedrijven hun sleutelbeheerprocessen verbeteren om dergelijke inbreuken te voorkomen.

## Kwetsbaarheden in algoritmen

Cryptografische algoritmen en protocollen kunnen kwetsbaarheden bevatten. Nieuwe technologieën kunnen deze blootleggen, waardoor versleutelde berichten kunnen worden ontcijferd. Daarom is het belangrijk dat we deze systemen voortdurend blijven verbeteren om onze digitale communicatie en gegevens veilig te houden.

## Kwantumcomputers

Kwantumcomputers vormen een potentieel risico voor cryptografie. Ze kunnen in theorie veel van de huidige cryptografische algoritmen kraken door hun vermogen om meerdere berekeningen tegelijk uit te voeren [4]. Dit kan leiden tot het ontcijferen van versleutelde informatie die bedoeld is om privé te blijven. Daarom is er een groeiende interesse in post-kwantum cryptografie, die algoritmen ontwikkelt die bestand zijn tegen kwantumaanvallen. Het is een actief onderzoeksgebied dat van cruciaal belang is voor de toekomstige beveiliging van onze digitale wereld.

## Conclusie

Cryptografie, wordt geconfronteerd met verschillende huidige en opkomende bedreigingen. Deze omvatten kwetsbaarheden in cryptografische algoritmen, uitdagingen in sleutelbeheer en de potentiële impact van kwantumcomputers. Het veilig opslaan van privésleutels en het voortdurend verbeteren van cryptografische systemen zijn cruciaal om deze bedreigingen het hoofd te bieden. Bovendien benadrukt de opkomst van kwantumcomputers de noodzaak om te investeren in post-kwantum cryptografie. Het is duidelijk dat, terwijl we de voordelen van cryptografie benutten, we ook proactief moeten zijn in het aanpakken van deze uitdagingen om de integriteit en veiligheid van onze digitale communicatie en gegevens te waarborgen.

# Ethische en maatschappelijke implicaties

Cryptografie speelt een cruciale rol in de bescherming van informatie en het waarborgen van privacy. Echter, naast de technische aspecten, roept het gebruik van cryptografie ook belangrijke ethische en maatschappelijke vragen op. Deze paragraaf zal deze kwesties onderzoeken, waarbij zowel de positieve als de potentieel problematische implicaties van cryptografie worden belicht. Van de bescherming van individuele privacy tot de mogelijkheid van misbruik voor illegale doeleinden, en van het versterken van digitale veiligheid tot het creëren van nieuwe uitdagingen voor wetshandhaving.

## Waarborgen van privacy

Privacy is een fundamenteel recht dat door cryptografie kan worden versterkt [5]. Door gegevens te versleutelen, kunnen individuen en organisaties hun informatie beschermen tegen ongewenste toegang. Echter, kan dit ook een tweesnijdend zwaard zijn. Terwijl het de privacy beschermt, kan cryptografie ook worden gebruikt om illegale activiteiten te verbergen, wat uitdagingen oplevert voor wetshandhaving en nationale veiligheid.

## Verkrijgen van toegang tot versleutelde communicatie

Cryptografie, hoewel een krachtig hulpmiddel voor het waarborgen van privacy en veiligheid, roept ook belangrijke ethische vragen op, voornamelijk met betrekking tot de toegang van overheidsinstanties tot versleutelde informatie. Overheidsinstanties hebben vaak toegang tot informatie nodig voor legitieme doeleinden, zoals nationale veiligheid of strafrechtelijk onderzoek. Echter, ongecontroleerde toegang kan leiden tot misbruik van macht en inbreuk op de privacy. Het vinden van een evenwicht tussen deze tegenstrijdige behoeften is een complexe ethische uitdaging.

## Evenwicht tussen veiligheid en privacy

Het discussiepunt rondom ‘achterdeuren’ in versleutelde systemen belicht dit vraagstuk [6]. Aan de ene kant zijn er mensen die voorstander zijn van dergelijke achterdeuren om toegang te krijgen tot versleutelde data, terwijl er aan de andere kant zorgen zijn over de gevolgen voor de privacy.

## Conclusie

Op basis van de besproken punten kunnen we concluderen dat cryptografie een krachtig hulpmiddel is dat zowel positieve als potentieel problematische implicaties heeft. Hoewel het de privacy en veiligheid kan versterken, roept het ook belangrijke ethische en maatschappelijke vragen op. De mogelijkheid van misbruik voor illegale doeleinden en de uitdagingen voor wetshandhaving en nationale veiligheid zijn belangrijke overwegingen. Bovendien is de toegang van overheidsinstanties tot versleutelde informatie een complexe ethische uitdaging. Het vinden van een evenwicht tussen deze tegenstrijdige behoeften - het waarborgen van privacy en veiligheid, het voorkomen van misbruik, en het mogelijk maken van legitieme toegang voor overheidsinstanties - is een cruciale taak voor onze samenleving.

# Conclusie

Hoofdvraag: “Op welke manier kan cryptografie worden toegepast om de veiligheid en privacy van digitale communicatie te waarborgen binnen een evoluerende technologische omgeving?”

Na analyse van de deelconclusies, wordt het duidelijk dat er een patroon van balans is tussen de uitdagingen en voordelen. Een specifiek voorbeeld hiervan is het ethische dilemma tussen privacy en veiligheid bij de toegang tot versleutelde informatie om illegale activiteiten tegen te gaan.

Cryptografie kan effectief worden toegepast om privacy en veiligheid te behouden, mits er een grondig begrip is van de basisprincipes en een bewustzijn van de opkomende bedreigingen. Dit vereist dat cryptografie zich blijft ontwikkelen en aanpassen aan het veranderende technologische landschap.

Voor toekomstig onderzoek zou het nuttig zijn om dieper in te gaan op specifieke bedreigingen en uitdagingen die in de tweede deelvraag zijn besproken. Dit zou kunnen omvatten het onderzoeken van mogelijke oplossingen voor deze bedreigingen.

Daarnaast zou het interessant kunnen zijn om dieper in te gaan op het ethische aspect van cryptografie. In dit onderzoek hebben we mogelijke problematische implicaties besproken, maar nog geen oplossingen geboden. Het onderzoeken van mogelijke oplossingen voor deze ethische vraagstukken zou een waardevolle aanvulling kunnen zijn op toekomstig onderzoek.

# Literatuurlijst

[1] [Kotzanikolaou, P., & Douligeris, C. (2007). Cryptography Primer: Introduction to Cryptographic Principles and Algorithms. *Network Security: Current Status and Future Directions, Edited by C. Douligeris and DN Serpanos, IEEE Press*, 459-479.](https://d1wqtxts1xzle7.cloudfront.net/66667487/9780470099742-libre.pdf?1619293806=&response-content-disposition=inline%3B+filename%3DAppendix_A_Cryptography_Primer_Introduct.pdf&Expires=1716976766&Signature=Fnln-B2eYXgbaWw4DSwUWUc-3p2bDhtH6sWi85-ISgNCAe~erwZ9kHZeNpHoSVjOe4qRzilsz76C3dKcmxn0EK3kkl7HklSdm6IyLKG9fzMmWvXEMY0-3SgJFeiqHnn74eiSlrDPpRBcERezO6kFKiPNNukfVmMMX7MiN0TBpGkcfWgpdMtVvjwFRFsr8NI~45AQxwdVlVG3iwwBoYWMyGyOnX~t9GmaRN5p5O8Y5I1kjoa0m-SXlZhfY0~5bqop6TA0zOuOuLh6IRNgtVDPm4VAdaSFu7ZY1SpA0a2kC-6KwBy18N3lls7SObdgAOt7Hv1Vu4tQd6NBAOyqpJo5Gg__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA)

[2] [PGP Corporation. (2002). An Introduction to cryptography. In An Introduction to Cryptography.](https://www.cs.unibo.it/babaoglu/courses/security/resources/documents/intro-to-crypto.pdf)  
  
[3] [Rana, S., Parast, F. K., Kelly, B., Wang, Y., & Kent, K. B. (2023). A comprehensive survey of cryptography key management systems. Journal of Information Security and Applications, 78, 103607.](https://doi.org/10.1016/j.jisa.2023.103607)

[4] [Kong, I., Janssen, M., & Bharosa, N. (2022). Challenges in the Transition towards a Quantum-safe Government. In Proceedings of the 23rd Annual International Conference on Digital Government Research. DOI: 10.1145/3543434.3533644](https://pure.tudelft.nl/ws/portalfiles/portal/133816997/3543434.3543644.pdf)

[5] [Shearer, J., & Gutmann, P. (1996). Government, cryptography, and the right to privacy. *Journal of Universal Computer Science*, *2*(3), 113-146.](https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=f9a3fc125279180f2982bd246a673f5bf1cf9917)

[6] [Martin, J. A. (2017). Encryption Backdoors: A Discussion of Feasibility, Ethics, and the Future of Cryptography.](https://digitalcommons.spu.edu/cgi/viewcontent.cgi?article=1062&context=honorsprojects)