Quantencomputer und Kryptografie: Warum heutige Sicherheit morgen brüchig sein kann

C2.1 - QUANTENTECHNOLOGIEN UND SICHERHEIT: WENN VERSCHLÜSSELUNG VERALTET

Wortschatz zum Text

Deutsch	Englisch / Erklärung
die Quantentechnologie	quantum technology
der Quantencomputer	quantum computer
die Kryptografie	cryptography
die Verschlüsselung	encryption
der Schlüssel	key
der öffentliche Schlüssel	public key
der private Schlüssel	private key
das asymmetrische Verfahren	asymmetric method
das symmetrische Verfahren	symmetric method
die Primfaktorzerlegung	prime factorization
der diskrete Logarithmus	discrete logarithm
die Rechenkomplexität	computational complexity
die Sicherheitsannahme	security assumption
die Schlüssellänge	key length
die Entschlüsselung	decryption
die Geheimhaltung	confidentiality
die Integrität	integrity
die Authentizität	authenticity
die digitale Signatur	digital signature
das Zertifikat	certificate

Deutsch	Englisch / Erklärung
die Zertifizierungsstelle	certificate authority
die Public-Key-Infrastruktur	public key infrastructure
der Angriffsvektor	attack vector
die Sicherheitslücke	security vulnerability
die Bedrohungsmodellierung	threat modeling
die Migrationsstrategie	migration strategy
die Übergangsphase	transition phase
die Standardisierung	standardization
die Implementierung	implementation
die Rückwärtskompatibilität	backward compatibility
die Schlüsselverteilung	key distribution
die Kommunikationssicherheit	communication security
die Langzeitvertraulichkeit	long-term confidentiality
die Risikobewertung	risk assessment
die Angriffsfläche	attack surface
die Rechenleistung	computing power
die Fehlertoleranz	fault tolerance
die Quantenüberlegenheit	quantum advantage
die Kryptoagilität	crypto-agility
die Post-Quanten-Kryptografie	post-quantum cryptography
der Algorithmuswechsel	algorithm change
die Vertrauensinfrastruktur	trust infrastructure
der Sicherheitsstandard	security standard
die Abhörsicherheit	eavesdropping resistance
die Schlüsselvereinbarung	key agreement
die mathematische Härte	mathematical hardness
die Skalierbarkeit	scalability
die Verwundbarkeit	vulnerability

Deutsch	Englisch / Erklärung
die Zukunftssicherheit	future-proof security
die Übergangsarchitektur	transition architecture
die Sicherheitsgarantie	security guarantee
die Kompromittierung	compromise
die Angriffskosten	attack costs
die technische Reife	technological maturity
quantenresistent	quantum-resistant
kryptografisch	cryptographic
angreifbar	vulnerable
skalierbar	scalable
fehlerkorrigiert	error-corrected

Meine zusätzlichen Wörter / Notizen:

Quantencomputer und Kryptografie: Warum heutige Sicherheit morgen brüchig sein kann

C2.1 - QUANTENTECHNOLOGIEN UND SICHERHEIT: WENN VERSCHLÜSSELUNG VERALTET

Digitale Sicherheit beruht auf einem stillen Vertrauen: dass bestimmte mathematische Aufgaben für Angreifer praktisch unlösbar sind. Wenn ein Browser eine verschlüsselte Verbindung aufbaut, wenn eine Banktransaktion signiert wird oder wenn ein Softwareupdate als echt überprüft wird, arbeiten im Hintergrund kryptografische Verfahren. Diese Verfahren verstecken nicht einfach Informationen hinter einem Passwort. Sie stützen sich auf präzise Annahmen darüber, welche Berechnungen mit verfügbaren Computern realistisch möglich sind und welche nicht. Genau hier entsteht das Problem der Quantentechnologien: Sie verändern nicht die Logik aller Sicherheit, aber sie stellen einige ihrer wichtigsten Annahmen infrage.

Besonders betroffen ist die asymmetrische Kryptografie. Bei ihr gibt es einen öffentlichen Schlüssel, den andere nutzen dürfen, und einen privaten Schlüssel, der geheim bleiben muss. Dieses Prinzip ermöglicht sichere Kommunikation zwischen Parteien, die vorher keinen gemeinsamen geheimen Schlüssel ausgetauscht haben. Es ist die Grundlage vieler digitaler Infrastrukturen: verschlüsselte Webseiten, digitale Signaturen, Zertifikate, E-Mail-Sicherheit, Softwareverteilung und Identitätsprüfung. Die Sicherheit vieler solcher Verfahren beruht darauf, dass bestimmte mathematische Probleme, etwa Primfaktorzerlegung oder diskrete Logarithmen, für klassische Computer extrem schwer zu lösen sind.

Ein leistungsfähiger Quantencomputer könnte diese Annahme unter bestimmten Bedingungen brechen. Entscheidend ist dabei nicht irgendein kleines experimentelles Quantengerät, sondern ein skalierbarer, fehlerkorrigierter Quantencomputer mit genügend stabilen Recheneinheiten. Der Unterschied ist wichtig: Nicht jede Meldung über Fortschritte in der Quantenforschung bedeutet, dass heutige Verschlüsselung morgen zusammenbricht. Doch ebenso falsch wäre es, das Risiko zu ignorieren, nur weil die technische Reife noch nicht erreicht ist. Sicherheitsarchitektur muss nicht erst reagieren, wenn ein Angriff bereits praktisch demonstriert wurde.

Kryptografische Sicherheit ist immer zeitabhängig. Ein Verfahren kann heute sicher sein und in zehn oder zwanzig Jahren problematisch werden. Das gilt auch ohne Quantencomputer, etwa wenn Rechenleistung wächst oder Implementierungsfehler entdeckt werden. Quantentechnologien verschärfen diese Zeitfrage jedoch, weil sie nicht nur Schlüssellängen anpassen, sondern ganze Klassen von Verfahren entwerten könnten. Wenn das zugrunde liegende mathematische Problem nicht mehr hart genug ist, hilft es nur begrenzt, den Schlüssel länger zu machen. Dann braucht es andere Verfahren mit anderen Sicherheitsannahmen.

Dabei betrifft die Gefahr nicht nur zukünftige Kommunikation. Besonders sensibel ist Langzeitvertraulichkeit. Manche Daten müssen nicht nur heute, sondern über Jahrzehnte geschützt bleiben: Gesundheitsdaten, diplomatische Kommunikation, Forschungsdaten, Geschäftsgeheimnisse, militärische Informationen oder personenbezogene Archive. Wenn solche Daten heute abgefangen und gespeichert werden, könnten sie später entschlüsselt werden, sobald geeignete Technik verfügbar ist. Sicherheit muss daher die Lebensdauer des Geheimnisses berücksichtigen, nicht nur den aktuellen Stand der Angreifer.

Anders ist die Lage bei digitalen Signaturen. Hier geht es weniger darum, vergangene Nachrichten geheim zu halten, sondern darum, Echtheit und Integrität nachzuweisen. Wenn ein Signaturverfahren gebrochen wird, könnten gefälschte Softwareupdates, manipulierte Zertifikate oder nachträglich erzeugte Dokumente vertrauenswürdig erscheinen. Die Folgen wären nicht nur technische Fehler, sondern Vertrauenskrisen in ganze Infrastrukturen. Eine Public-Key-Infrastruktur lebt davon, dass Zertifikate, Schlüssel und Signaturen als verlässlich gelten. Wird diese Vertrauensordnung erschüttert, reicht es nicht, einzelne Dateien neu zu verschlüsseln.

Post-Quanten-Kryptografie versucht, Verfahren zu entwickeln, die auch gegenüber bekannten Quantenangriffen sicher bleiben sollen. Dabei geht es nicht darum, Quantenphysik zur Verschlüsselung zu verwenden, sondern um klassische Algorithmen, deren Sicherheitsannahmen nach heutigem Wissen nicht durch Quantencomputer gebrochen werden. Diese Unterscheidung wird häufig übersehen. Quantenkommunikation, Quantencomputer und Post-Quanten-Kryptografie sind verwandte, aber nicht identische Felder. Für die breite digitale Infrastruktur ist besonders wichtig, Verfahren zu finden, die auf heutigen Computern funktionieren und dennoch zukünftigen Quantenangriffen standhalten.

Der Übergang ist jedoch nicht einfach ein technisches Update. Kryptografie steckt tief in Protokollen, Geräten, Betriebssystemen, Chips, Karten, Servern, Archiven und Verwaltungsprozessen. Manche Systeme werden jahrelang nicht aktualisiert, manche Geräte sind eingebettet und schwer zugänglich, manche Zertifikatsketten hängen von internationalen Standards ab. Ein Algorithmuswechsel muss getestet, standardisiert, implementiert und in bestehende Infrastrukturen integriert werden. Dabei können neue Fehler entstehen. Ein theoretisch starkes Verfahren hilft wenig, wenn es schlecht eingebaut wird.

Deshalb gewinnt Kryptoagilität an Bedeutung. Sie bezeichnet die Fähigkeit eines Systems, kryptografische Verfahren kontrolliert austauschen zu können, ohne die gesamte Infrastruktur neu aufzubauen. Ein kryptoagiles System ist nicht an einen einzigen Algorithmus gekettet. Es kann auf neue Standards reagieren, Übergangsphasen unterstützen und alte Verfahren ausmustern. Diese Fähigkeit klingt unspektakulär, ist aber strategisch entscheidend. Wer heute starre Systeme baut, schafft morgen Migrationsprobleme.

Die größte Schwierigkeit liegt nicht darin, dass niemand das Risiko kennt. Sie liegt darin, dass der Zeitpunkt unsicher ist. Wenn eine Bedrohung morgen sicher eintreten würde, wäre politisches Handeln leichter zu begründen. Wenn sie nie eintritt, wirken Investitionen übertrieben. Quantenbedrohungen liegen genau dazwischen: ernst genug, um vorbereitet zu werden, aber unsicher genug, um Verdrängung zu begünstigen. Sicherheitsplanung muss daher mit Unsicherheit umgehen, statt sie als Ausrede für Untätigkeit zu verwenden.

Auch die Verantwortung ist verteilt. Forschungseinrichtungen entwickeln und prüfen neue Verfahren. Standardisierungsorganisationen legen Empfehlungen fest. Unternehmen müssen Produkte aktualisieren. Behörden müssen kritische Infrastrukturen priorisieren. Betreiber müssen wissen, welche Daten Langzeitschutz brauchen. Nutzerinnen und Nutzer sehen von all dem meist nur ein Schloss-Symbol im Browser. Doch dieses Symbol ist nur die Oberfläche einer komplexen Vertrauensarchitektur.

Quantencomputer machen Verschlüsselung nicht grundsätzlich unmöglich. Sie zwingen aber dazu, Sicherheit weniger statisch zu denken. Ein sicheres System ist nicht eines, das für immer denselben Algorithmus nutzt, sondern eines, das seine Annahmen überprüft, seine Abhängigkeiten kennt und rechtzeitig migrieren kann. Die eigentliche Lehre lautet daher nicht: Alle heutige Sicherheit ist wertlos. Sie lautet: Sicherheit ist eine historische Praxis. Was heute robust ist, kann morgen brüchig werden, wenn die Welt, gegen die es schützen soll, sich verändert.

Fragen zum Text

1. Worauf beruht digitale Sicherheit laut Text in vielen Fällen?

2. Warum ist asymmetrische Kryptografie besonders wichtig?

3. Welche digitalen Infrastrukturen hängen von asymmetrischer Kryptografie ab?

4. Warum ist nicht jedes Quantengerät eine unmittelbare Gefahr für heutige Verschlüsselung?

5. Warum darf man die Quantenbedrohung dennoch nicht ignorieren?

6. Warum reicht eine bloße Verlängerung von Schlüsseln nicht immer aus?

7. Was bedeutet Langzeitvertraulichkeit?

8. Warum sind heute abgefangene Daten ein zukünftiges Risiko?

9. Warum sind digitale Signaturen anders betroffen als verschlüsselte Nachrichten?

10. Welche Folgen hätte ein gebrochenes Signaturverfahren?

11. Was ist Post-Quanten-Kryptografie?

12. Warum ist Post-Quanten-Kryptografie nicht dasselbe wie Quantenkommunikation?

13. Warum ist die Umstellung auf neue Kryptografie kein einfaches Update?

14. Was bedeutet Kryptoagilität?

15. Warum erschwert Unsicherheit den politischen Umgang mit Quantenrisiken?

16. Warum ist Verantwortung in dieser Frage verteilt?

17. Was ist die zentrale Schlussfolgerung des Textes?

Multiple Choice

1. Was stellt Quantencomputing bei heutiger Kryptografie besonders infrage?

- [ ] A) Die Annahme, dass bestimmte mathematische Probleme praktisch schwer lösbar sind.
- [ ] B) Die Existenz aller Passwörter.
- [ ] C) Die Notwendigkeit von Softwareupdates.
- [ ] D) Die Möglichkeit jeder digitalen Kommunikation.

2. Warum ist asymmetrische Kryptografie besonders verwundbar?

- [ ] A) Viele Verfahren beruhen auf mathematischen Problemen, die durch leistungsfähige Quantencomputer angreifbar werden könnten.
- [ ] B) Sie verwendet niemals Schlüssel.
- [ ] C) Sie schützt keine öffentlichen Dienste.
- [ ] D) Sie funktioniert nur ohne Computer.

3. Welche Aussage ist texttreu?

- [ ] A) Jedes heutige Quantengerät kann sofort alle Verschlüsselung brechen.
- [ ] B) Relevant wäre ein skalierbarer, fehlerkorrigierter Quantencomputer.
- [ ] C) Quantencomputer betreffen nur Bildschirmhelligkeit.
- [ ] D) Kryptografie ist unabhängig von Rechenmodellen.

4. Warum ist Langzeitvertraulichkeit wichtig?

- [ ] A) Manche Daten müssen auch in Jahrzehnten noch geheim bleiben.
- [ ] B) Alle Daten verlieren nach einem Tag ihren Wert.
- [ ] C) Verschlüsselung schützt nur Live-Chats.
- [ ] D) Gesundheitsdaten sind nie langfristig sensibel.

5. Was ist das Risiko gespeicherter verschlüsselter Daten?

- [ ] A) Sie könnten heute gesammelt und später entschlüsselt werden.
- [ ] B) Sie löschen sich automatisch.
- [ ] C) Sie sind ohne Schlüssel immer öffentlich.
- [ ] D) Sie haben keine Beziehung zu Quantencomputern.

6. Warum sind Signaturen besonders kritisch?

- [ ] A) Sie sichern Echtheit und Integrität digitaler Objekte.
- [ ] B) Sie komprimieren Bilder.
- [ ] C) Sie speichern Passwörter im Klartext.
- [ ] D) Sie ersetzen jede Infrastruktur.

7. Was bedeutet Post-Quanten-Kryptografie?

- [ ] A) Klassische kryptografische Verfahren mit Widerstand gegen bekannte Quantenangriffe.
- [ ] B) Verschlüsselung, die nur auf Quantencomputern läuft.
- [ ] C) Das Ende aller Standards.
- [ ] D) Ein Verbot digitaler Signaturen.

8. Warum ist Kryptoagilität wichtig?

- [ ] A) Systeme müssen Algorithmen austauschen können.
- [ ] B) Sie verhindert jede Standardisierung.
- [ ] C) Sie macht Bedrohungsmodelle überflüssig.
- [ ] D) Sie erlaubt nie Übergangsphasen.

9. Was ist die größte planerische Schwierigkeit?

- [ ] A) Der Zeitpunkt praktischer Quantenangriffe ist unsicher.
- [ ] B) Es gibt keine betroffenen Systeme.
- [ ] C) Alle Geräte aktualisieren sich automatisch.
- [ ] D) Niemand kennt kryptografische Verfahren.

10. Welche Schlussfolgerung passt zum Text?

- [ ] A) Sicherheit ist kein statischer Zustand, sondern eine anpassungsfähige Praxis.
- [ ] B) Alle heutige Verschlüsselung ist sofort wertlos.
- [ ] C) Migration kann beliebig lange warten.
- [ ] D) Quantencomputer machen Geheimhaltung grundsätzlich unmöglich.

Ordne zu

A	B
Asymmetrische Kryptografie	ermöglicht Kommunikation ohne vorher geteiltes Geheimnis.
Öffentlicher Schlüssel	darf verteilt werden.
Privater Schlüssel	muss geheim bleiben.
Primfaktorzerlegung	ist eine klassische Sicherheitsannahme bestimmter Verfahren.
Diskreter Logarithmus	gehört zu den mathematisch relevanten Problemen.
Quantencomputer	könnten bestimmte Annahmen klassischer Verfahren schwächen.
Fehlerkorrektur	ist für skalierbare Quantenangriffe entscheidend.
Langzeitvertraulichkeit	betrifft Daten mit langem Schutzbedarf.
Digitale Signaturen	sichern Echtheit und Integrität.
Zertifikate	gehören zur Vertrauensinfrastruktur.
Public-Key-Infrastruktur	organisiert Vertrauen in Schlüssel und Identitäten.
Post-Quanten-Kryptografie	nutzt klassische Verfahren gegen Quantenbedrohungen.
Quantenkommunikation	ist nicht identisch mit Post-Quanten-Kryptografie.
Algorithmuswechsel	erfordert Tests, Standards und Implementierung.
Rückwärtskompatibilität	kann Migration verlangsamen.
Kryptoagilität	erlaubt kontrollierten Austausch von Verfahren.
Sicherheitsannahmen	müssen regelmäßig überprüft werden.
Implementierungsfehler	können starke Verfahren praktisch schwächen.
Bedrohungsmodellierung	berücksichtigt Gegner, Zeiträume und Schutzbedarf.
Standardisierung	schafft gemeinsame Grundlage für Umstellung.
Kritische Infrastruktur	braucht Priorisierung bei der Migration.
Übergangsphase	kann alte und neue Verfahren parallel enthalten.

A	B
Angriffskosten	bestimmen praktische Machbarkeit.
Zukunftssicherheit	hängt von Anpassungsfähigkeit ab.
Vertrauensarchitektur	bleibt für Nutzer oft unsichtbar.
Kompromittierung	kann einzelne Schlüssel oder ganze Verfahren betreffen.
Technische Reife	entscheidet über zeitliche Dringlichkeit.
Verwundbarkeit	entsteht aus falschen oder veralteten Annahmen.

Bringe in die richtige Reihenfolge

Nr.	Satz / Ereignis	Reihenfolge
1.	Danach wird asymmetrische Kryptografie als Grundlage digitaler Infrastruktur erklärt.	
2.	Der Text beginnt mit der Sicherheitsannahme mathematischer Schwierigkeit.	
3.	Später wird Langzeitvertraulichkeit als besonderes Risiko beschrieben.	
4.	Anschließend wird die mögliche Wirkung leistungsfähiger Quantencomputer eingeordnet.	
5.	Zum Schluss wird Sicherheit als historische und anpassungsfähige Praxis verstanden.	
6.	Danach wird betont, dass nicht jedes Quantengerät unmittelbare Gefahr bedeutet.	
7.	Es wird erklärt, warum ganze Klassen von Verfahren betroffen sein können.	
8.	Der Text unterscheidet anschließend Geheimhaltung und digitale Signaturen.	
9.	Später wird Post-Quanten-Kryptografie von Quantenkommunikation abgegrenzt.	
10.	Danach wird der Übergang als komplexe Infrastrukturaufgabe beschrieben.	
11.	Ein weiterer Schritt ist die Einführung von Kryptoagilität.	
12.	Danach wird Unsicherheit über den Zeitpunkt als Planungsproblem analysiert.	
13.	Der Text beschreibt die verteilte Verantwortung verschiedener Akteure.	
14.	Am Ende wird das Browser-Symbol als Oberfläche einer Vertrauensarchitektur verstanden.	
15.	Die Rolle von Zertifikaten und Signaturen wird als Vertrauensproblem dargestellt.	
16.	Die Notwendigkeit anderer Sicherheitsannahmen wird erläutert.	
17.	Es folgt die Warnung vor starren Systemen ohne Migrationsfähigkeit.	

Nr.	Satz / Ereignis	Reihenfolge
18.	Der Text macht deutlich, dass Quantencomputer Verschlüsselung nicht grundsätzlich unmöglich machen.	

Finde den Fehler im Inhalt

1. Digitale Sicherheit beruht laut Text ausschließlich auf geheimen Passwörtern.

2. Asymmetrische Kryptografie benötigt immer einen vorher gemeinsam ausgetauschten geheimen Schlüssel.

3. Jeder heutige Quantenchip kann sofort alle digitalen Signaturen brechen.

4. Quantenrisiken sind irrelevant, solange noch kein praktischer Angriff demonstriert wurde.

5. Bei gebrochenen mathematischen Grundannahmen reicht es immer, denselben Schlüssel etwas länger zu machen.

6. Langzeitvertraulichkeit betrifft nur Nachrichten, die morgen gelöscht werden.

7. Digitale Signaturen schützen vor allem die Geheimhaltung alter Nachrichten.

8. Post-Quanten-Kryptografie bedeutet, dass nur Quantencomputer verschlüsseln können.

9. Die Umstellung auf quantenresistente Verfahren ist ein einfaches Update ohne Risiken.

10. Kryptoagilität bedeutet, dass ein System dauerhaft an einen einzigen Algorithmus gebunden bleibt.

11. Der genaue Zeitpunkt der Quantenbedrohung ist vollständig bekannt.

12. Nur Endnutzerinnen und Endnutzer tragen Verantwortung für die Migration.

13. Quantencomputer machen jede Form digitaler Sicherheit unmöglich.

14. Ein sicheres System muss seinen Algorithmus niemals überprüfen.

15. Das Schloss-Symbol im Browser zeigt die ganze Komplexität digitaler Sicherheit vollständig.

Schreibaufgabe

320-380 Wörter

Analysiere, warum Quantencomputer nicht einfach „das Ende der Verschlüsselung“ bedeuten, aber dennoch eine grundlegende Herausforderung für digitale Sicherheitsarchitekturen darstellen. Gehe auf asymmetrische Kryptografie, Langzeitvertraulichkeit, digitale Signaturen, Post-Quanten-Kryptografie, Kryptoagilität und Migrationsrisiken ein.

Lösungen

Fragen zum Text

1. Sie beruht auf der Annahme, dass bestimmte mathematische Aufgaben für Angreifer praktisch unlösbar sind.
2. Sie ermöglicht sichere Kommunikation und digitale Signaturen ohne vorher geteilten geheimen Schlüssel.
3. Verschlüsselte Webseiten, Zertifikate, digitale Signaturen, E-Mail-Sicherheit, Softwareverteilung und Identitätsprüfung hängen davon ab.
4. Gefährlich wäre vor allem ein skalierbarer, fehlerkorrigierter Quantencomputer mit genügend stabiler Rechenleistung.
5. Sicherheitsarchitektur muss vorbereitet werden, bevor ein Angriff praktisch demonstriert und massenhaft nutzbar ist.
6. Wenn das zugrunde liegende mathematische Problem durch Quantenverfahren grundsätzlich leichter lösbar wird, braucht man andere Sicherheitsannahmen.
7. Daten müssen nicht nur heute, sondern über viele Jahre oder Jahrzehnte geheim bleiben.
8. Sie können gespeichert und später entschlüsselt werden, wenn geeignete Quantencomputer verfügbar sind.
9. Bei Signaturen geht es vor allem um Echtheit und Integrität, nicht primär um Geheimhaltung vergangener Inhalte.
10. Gefälschte Softwareupdates, manipulierte Zertifikate oder falsche Dokumente könnten vertrauenswürdig erscheinen.
11. Sie entwickelt klassische Verfahren, die nach heutigem Wissen auch gegen bekannte Quantenangriffe widerstandsfähig sein sollen.
12. Post-Quanten-Kryptografie nutzt klassische Algorithmen, während Quantenkommunikation physikalische Quanteneffekte verwendet.
13. Kryptografie ist tief in Protokollen, Geräten, Chips, Betriebssystemen, Zertifikaten und Verwaltungsprozessen eingebettet.
14. Kryptoagilität bedeutet, kryptografische Verfahren kontrolliert austauschen zu können, ohne die gesamte Infrastruktur neu aufzubauen.
15. Der genaue Zeitpunkt praktischer Angriffe ist unklar, wodurch Investitionen leicht aufgeschoben oder als übertrieben dargestellt werden.
16. Forschung, Standardisierung, Unternehmen, Behörden, Betreiber kritischer Infrastrukturen und Nutzer tragen jeweils unterschiedliche Verantwortung.
17. Sicherheit muss historisch und dynamisch gedacht werden, weil heute robuste Verfahren morgen brüchig werden können.

Multiple Choice

1. A) Die Annahme, dass bestimmte mathematische Probleme praktisch schwer lösbar sind.
2. A) Viele Verfahren beruhen auf mathematischen Problemen, die durch leistungsfähige Quantencomputer angreifbar werden könnten.
3. B) Relevant wäre ein skalierbarer, fehlerkorrigierter Quantencomputer.
4. A) Manche Daten müssen auch in Jahrzehnten noch geheim bleiben.

Lösungen

Multiple Choice (Fortsetzung)

5. A) Sie könnten heute gesammelt und später entschlüsselt werden.
6. A) Sie sichern Echtheit und Integrität digitaler Objekte.
7. A) Klassische kryptografische Verfahren mit Widerstand gegen bekannte Quantenangriffe.
8. A) Systeme müssen Algorithmen austauschen können.
9. A) Der Zeitpunkt praktischer Quantenangriffe ist unsicher.
10. A) Sicherheit ist kein statischer Zustand, sondern eine anpassungsfähige Praxis.

Zuordnung

1. 1. Asymmetrische Kryptografie — ermöglicht Kommunikation ohne vorher geteiltes Geheimnis.
2. 2. Öffentlicher Schlüssel — darf verteilt werden.
3. 3. Privater Schlüssel — muss geheim bleiben.
4. 4. Primfaktorzerlegung — ist eine klassische Sicherheitsannahme bestimmter Verfahren.
5. 5. Diskreter Logarithmus — gehört zu den mathematisch relevanten Problemen.
6. 6. Quantencomputer — könnten bestimmte Annahmen klassischer Verfahren schwächen.
7. 7. Fehlerkorrektur — ist für skalierbare Quantenangriffe entscheidend.
8. 8. Langzeitvertraulichkeit — betrifft Daten mit langem Schutzbedarf.
9. 9. Digitale Signaturen — sichern Echtheit und Integrität.
10. 10. Zertifikate — gehören zur Vertrauensinfrastruktur.
11. 11. Public-Key-Infrastruktur — organisiert Vertrauen in Schlüssel und Identitäten.
12. 12. Post-Quanten-Kryptografie — nutzt klassische Verfahren gegen Quantenbedrohungen.
13. 13. Quantenkommunikation — ist nicht identisch mit Post-Quanten-Kryptografie.
14. 14. Algorithmuswechsel — erfordert Tests, Standards und Implementierung.
15. 15. Rückwärtskompatibilität — kann Migration verlangsamen.
16. 16. Kryptoagilität — erlaubt kontrollierten Austausch von Verfahren.
17. 17. Sicherheitsannahmen — müssen regelmäßig überprüft werden.
18. 18. Implementierungsfehler — können starke Verfahren praktisch schwächen.
19. 19. Bedrohungsmodellierung — berücksichtigt Gegner, Zeiträume und Schutzbedarf.
20. 20. Standardisierung — schafft gemeinsame Grundlage für Umstellung.
21. 21. Kritische Infrastruktur — braucht Priorisierung bei der Migration.

Lösungen

Zuordnung (Fortsetzung)

22. 22. Übergangsphase — kann alte und neue Verfahren parallel enthalten.
23. 23. Angriffskosten — bestimmen praktische Machbarkeit.
24. 24. Zukunftssicherheit — hängt von Anpassungsfähigkeit ab.
25. 25. Kompromittierung — kann einzelne Schlüssel oder ganze Verfahren betreffen.
26. 26. Vertrauensarchitektur — bleibt für Nutzer oft unsichtbar.
27. 27. Verwundbarkeit — entsteht aus falschen oder veralteten Annahmen.
28. 28. Technische Reife — entscheidet über zeitliche Dringlichkeit.

Reihenfolge

1. 1. Der Text beginnt mit der Sicherheitsannahme mathematischer Schwierigkeit.
2. 2. Danach wird asymmetrische Kryptografie als Grundlage digitaler Infrastruktur erklärt.
3. 3. Anschließend wird die mögliche Wirkung leistungsfähiger Quantencomputer eingeordnet.
4. 4. Danach wird betont, dass nicht jedes Quantengerät unmittelbare Gefahr bedeutet.
5. 5. Es wird erklärt, warum ganze Klassen von Verfahren betroffen sein können.
6. 6. Die Notwendigkeit anderer Sicherheitsannahmen wird erläutert.
7. 7. Später wird Langzeitvertraulichkeit als besonderes Risiko beschrieben.
8. 8. Der Text unterscheidet anschließend Geheimhaltung und digitale Signaturen.
9. 9. Die Rolle von Zertifikaten und Signaturen wird als Vertrauensproblem dargestellt.
10. 10. Später wird Post-Quanten-Kryptografie von Quantenkommunikation abgegrenzt.
11. 11. Danach wird der Übergang als komplexe Infrastrukturaufgabe beschrieben.
12. 12. Ein weiterer Schritt ist die Einführung von Kryptoagilität.
13. 13. Es folgt die Warnung vor starren Systemen ohne Migrationsfähigkeit.
14. 14. Danach wird Unsicherheit über den Zeitpunkt als Planungsproblem analysiert.
15. 15. Der Text beschreibt die verteilte Verantwortung verschiedener Akteure.
16. 16. Am Ende wird das Browser-Symbol als Oberfläche einer Vertrauensarchitektur verstanden.
17. 17. Der Text macht deutlich, dass Quantencomputer Verschlüsselung nicht grundsätzlich unmöglich machen.
18. 18. Zum Schluss wird Sicherheit als historische und anpassungsfähige Praxis verstanden.

Lösungen

Fehler finden

1. Sie beruht oft auf mathematischen Annahmen über praktisch schwer lösbare Aufgaben.
2. Sie nutzt öffentliche und private Schlüssel und ermöglicht Kommunikation ohne vorher geteiltes Geheimnis.
3. Entscheidend wäre ein skalierbarer, fehlerkorrigierter Quantencomputer mit ausreichender Rechenleistung.
4. Sicherheitsplanung muss vor praktischer Ausnutzung beginnen, besonders bei langen Migrationszeiten.
5. Wenn das zugrunde liegende Problem nicht mehr hart genug ist, braucht man andere Verfahren.
6. Sie betrifft Daten, die über Jahre oder Jahrzehnte geheim bleiben müssen.
7. Sie sichern Echtheit und Integrität von Daten, Software und Zertifikaten.
8. Sie bezeichnet klassische Verfahren, die gegen bekannte Quantenangriffe widerstandsfähig sein sollen.
9. Sie betrifft Protokolle, Geräte, Zertifikate, Standards und Implementierungen und kann neue Fehler erzeugen.
10. Kryptoagilität bedeutet, Verfahren kontrolliert austauschen zu können.
11. Er ist unsicher, was Planung und politische Priorisierung erschwert.
12. Verantwortung ist auf Forschung, Standardisierung, Unternehmen, Behörden, Betreiber und Nutzer verteilt.
13. Sie stellen bestimmte Verfahren infrage, machen Sicherheit aber nicht grundsätzlich unmöglich.
14. Ein sicheres System muss Annahmen überprüfen und bei Bedarf migrieren können.
15. Es zeigt nur die Oberfläche einer komplexen Vertrauensarchitektur.