Altfragenkatalog zu Einführung Kryptographie und IT-Sicherheit

Salzburg *21.12.2018*

1.) Diskutieren sie die verschiedenen Kategorien des "Brechens" eines Verschlüsselungs-Algorithmus. Zu welcher Kategorie gehört eine "timing-Attacke" ? Inwiefern ist die brute-force Attacke eine Schranke für die Sicherheit eines Algorithmus ? (2 Punkte)

2.) In welchem Verhältnis stehen IKE und IPSec (d.h. welche Aufgaben werden von welchem Verfahren übernommen) ? Inwiefern gibt es in der Struktur von SSH/TLS Ähnlichkeiten zu dieser Aufgabenverteilung ? (2 Punkte)

3.) Formulieren und begründen (mindestens 2 Gründe) sie das Kerckhoff'sche Prinzip und geben sie Beispiele aus der Realität für desaströse Verstösse und deren Konsequenzen. (2 Punkte)

4.) Welche 4 verschiedenen Attacken gegen kryptographische Protokolle wurden besprochen ? Erklären sie kurz wer diese Attacken durchführt. (2 Punkte)

5.) Erklären sie die Dictionary-Attacke gegen ein Authentifizierungssystem und warum die Verwendung von SALT (was ist das ?) diese Attacke schwieriger macht. Was wird bei der Verwendung von SALT beim PWD gespeichert ? Warum ist es also wichtig starke PWDs zu verwenden ? (2 Punkte)

6.) Berechnen sie die Wahrscheinlichkeit (und erklären sie ihre Berechnungsschritte) dass ein zufälliger Nachrichtenblock m_i nicht relativ prim zum RSA-Modul n ist. (2 Punkte)

7.) Im Zusammenhang mit RSA wurde eine Attacke gegen Verschlüsselung und Signierung besprochen, bei der die Grundidee ist, dass ein Angreifer einen passend gewählten neuen öffentlichen Exponenten wählt und publiziert um die Attacke zielgerichtet durchführen zu können. Erklären sie diese Attacke und geeignete Gegenmassnahmen. (2 Punkte)

8.) Erklären sie die Funktionsweise **und** beweisen sie schrittweise die Gültigkeit der digitalen Signatur nach El Gamal. Benennen sie ausserdem je einen Vor- und Nachteil verglichen mit RSA-basierten digitalen Signturen. (2 Punkte)

9.) Erklären sie die Funktionsweise des Cipher-block Chaining Modes für Blockcipher, Vor- und Nachteile gegenüber Electronic Codebook Mode und erklären sie genau warum es zur beschriebenen Fehlerausbreitung bei Ciphertextfehlern kommt (und auch warum diese "self recovering" ist). (2 Punkte)

10.) Erklären Sie anhand eines einfachen Protokolls den Diffie-Hellman Key-exchange Algorithmus. Wählen Sie $n = 7$ und rechnen Sie ein konkretes Beispiel durch. Was ist eine Primitivwurzel und warum ist deren Verwendung hier wichtig ? (2 Punkte)

11.) Wie funktioniert bei GSM Netzen die sichere Kommunikation zwischen Benutzer und Basisstation ? Welches Problem wird dabei unerfreulicherweise nicht gelöst ? (2 Punkte)

12.) Was ist multiple key public key cryptography und wie funktioniert das ? Für welche Anwendungsszenarien ist das von Vorteil (und welche konkreten Nachteile klassischer Ansätze werden dabei vermieden) ? (2 Punkte)

13.) Erklären Sie wie die Methode "counting coincidences" verwendet werden kann um die key-length bei Verschlüsselung mit XOR und einem kurzen Schüssel zu ermitteln. Begründen sie auch warum diese Methode funktioniert. Geben sie ein Beispiel für eine Methode der Entschlüsselung wenn die Schlüssellänge ermittelt wurde. (2 Punkte)

14.) Erklären die das Konzept von randomisierter Verschüsselung und wie dies bei Signaturen mit El Gamal angewendet wird. Was ist der Vorteil von RSA gegenüber dem Einsatz von El Gamal bei digitalen Signaturen ? (2 Punkte)

15.) Beschreiben sie detailliert eine der drei besprochenen Szenarien die darlegen, warum RSA nie benutzt werden darf um ein "zufällig" wirkendes Dokument zu signieren (chosen ciphertext Attacke). Erklären sie weiters (konkret anhand des gewählten Szenarios), was die Anwendung einer Hash-funktion bei der Signierung ändert (und ob das überhaupt etwas ändert). (2 Punkte)

16.) Erklären sie die Funktionsweise der S-Box Substitution in DES und vergleichen sie deren Funktionsweise mit der in AES verwendeten Substitution. In welcher Hinsicht besteht ein grundlegender Unterschied (bezogen auf die Substitution aber auch andere Elemente) zwischen den Designprinzipien von DES und AES ? (2 Punkte)

17.) Bleibt bei Substitution Ciphers oder Transposition Ciphers das Histogramm des Ciphertextes unverändert verglichen mit dem Histogramm des Plaintext ? Begründen sie ihre Antwort ! Welche Histogramm-basierte Attacke gibt es gegen Verschlüsselung (von Texten) mit Substitution Ciphers ? (2 Punkte)

18.) Was ist ein Message Authentication Code (MAC) ? Gibt es Unterschiede in der Funktionalität zur digitalen Signatur, wenn ja, inwiefern ? Beschreiben sie jeweilige Vor- und Nachteile ! Warum wird bei IPSec zur Authentifizierung ein MAC und keine digitale Signatur verwendet ? (2 Punkte)

19.) Erklären sie die Common Modulus Attacke gegen RSA und wie sie verhindert werden kann. (2 Punkte).

20.) Zum Verständnis von RSA: gegeben sind als public key $n = 21$ und $e = 5$. Sie fangen einen Ciphertext $c = 2$ ab. Ermitteln Sie durch eine Faktorisierungs-Attacke den dazugehörigen Plaintext und erklären Sie die Rolle der Faktorisierung bei Ihrer Attacke. (2 Punkte)

21.) Erklären Sie die Grundidee der Quantenkryptographie und warum es beim beschriebenen Verfahren möglich ist zu erkennen ob ein Lauscher am Kanal war (2 Punkte).

22.) Erklären Sie welche Bereiche der IP Pakete im Transport Mode beim ESP Protokoll von IP Secure authentifiziert bzw. verschlüsselt werden. Was ist Tunnel und Transport Mode ? Was ist der Unterschied zwischen ESP und AH ? (2 Punkte)

23.) Welches Problem wird bei SET durch sog. duale Signaturen gelöst und wie funktioniert das (z.B. bei der Bank wenn die Zahlungsinformation entschlüsselt wird) ? (2 Punkte)

24.) Wie funktioniert die Geburtstagsattacke gegen one-way Hash functions ? Worauf beruht sie ? Abhilfe ? (2 Punkte)

25.) Was ist eine Zero-Knowledge Protokoll und was ist der Unterschied zu z.B. klassischen Authentifizierungsprotokollen ? Beschreiben sie detailliert die Funktionsweise des Feige-Fiat Schamir Identifikations Schemas und erklären sie die zero-knowledge Eigenschaft. (3 Punkte)

26.) Erklären Sie warum bei OTP Verschüsselung ein OTP nur 1x als keystream verwendet werden darf. Welche Attacke wird ermöglicht wenn noch zusätzlich einer von zwei involvierten Plaintexten (die mit dem gleichen OTP verschlüsselt wurden) zur Verfügung steht ? (1 Punkt)

27.) Erklären Sie die Betriebsarten von Blockciphern (ECM, CBC, CFB, OFB), deren Vor- und Nachteile und ihr Verhalten bei Ciphertextfehlern bzgl Fehlerausbreitung. (2 Punkte)

28.) Was ist die "meet in the middle attack" (wie funktioniert sie) und was ist die Konsequenz ihrer Existenz ? (2 Punkte)

29.) Wie und warum können symmetrische Block-cipher verwendet werden um one-way Hash functions daraus zu bauen ? Erklären Sie anhand des Tandem Davies-Mayer Algorithmus konzeptuell wie unter Verwendung von AES ein sicherer 256 bit Hash erzeugt werden kann. (2 Punkte)

30.) Beschreiben Sie ein Verfahren und eine Anwendung von Secret Splitting für 2 und mehr Personen. Was ist der Unterschied zu Secret Sharing ? (1 Punkt)

31.) Erklären sie drei "computational infeasible problems" die die Grundlage von public key Verfahren bilden (auch warum das schwierige Probleme sind) **und** beschreiben sie in welcher Form sie bei je einem konkreten Algorithmus vorkommen (also warum sie konkret die Sicherheitsgrundlage dieser Verfahren bilden). (3 Punkte)

32.) Welcher Zahl im Restklassensystem Modulo 5 entspricht der Ausdruck $-\frac{7}{4} \pmod 5$? Erklären Sie die Berechnungsschritte. Bestimmen sie eine Primitivwurzel (was ist das ?) im Restklassensystem Modulo 5. (2 Punkte)

33.) Erklären Sie die wesentlichen Bestandteile eines Kerberos Realms und den Ablauf einer Applikationsanforderung und Durchführung. Wie wird inter-realm Authentifizierung realisiert ? Was sind Nachteile von Kerberos ? (2 Punkte)

34.) Welches grundsätzliche Problem der public-key Kryptographie muss für DNSSEC (auch) gelöst werden ? Wie wird das in DNSSEC gelöst ? Warum ist DNS Walking (was ist das ?) durch die Verwendung von NSEC3 RR nicht mehr möglich ? (2 Punkte)

35.) Wie und mit welchen kryptographischen Primitiven wird eine digitale Signatur typischerweise erstellt und wie wird sie verifiziert ? Erklären sie die Rolle der Komponenten und den Grund für ihre Verwendung. Geben sie konkrete Beispiele, welche Algorithmen für die verschiedenen Komponenten bei der Signaturerstellung verwendet werden können. (2 Punkte)

36.) Erklären sie was das diskrete Logarithmenproblem ist, bei welchen besprochenen Verfahren es die Sicherheitsgrundlage bildet und erklären sie intuitiv warum Logarithmieren in Restklassensystemen schwieriger ist als in klassischer Arithmetik. (2 Punkte)

37.) Erklären sie die Begriffe “Ciphertext-only Attacke” und “Known-Plaintext Attacke” und erklären sie genau, welches Wissen und welche Vorraussetzungen man für diese Attacken braucht. Gegen welche Art von Attacke sind Public-key Verfahren grundsätzlich immer anfällig und warum ? (2 Punkte)

38.) Erklären Sie die Grundprinzipien von elliptic curve cryptography, die Vor- und Nachteile, und die Anwendungsbereiche für die diese Verfahren besonders interessant sind. (2 Punkte)

39.) Wie könnte eine Mischung zwischen public key und symmetrischen Verfahren funktionieren (Stichwort hybride Verfahren) ? Warum ist so ein Verfahren sinnvoll ? (1 Punkt)

40.) Wie funktioniert das SKEY Authentifizierungssystem ? Inwiefern unterscheidet es sich von den meisten TAN-basierten Systemen beim electronic banking ? (1 Punkt)

41.) Erklären sie was eine “brute force attack” gegen einen cipher ist und unter welchen Bedingungen diese nicht erfolgreich anwendbar ist. (1 Punkt)

42.) Beschreiben sie die Funktionsweise, Funktionalitäten und Komponenten von PGP. (2 Punkte)

43.) Was ist die “man in the middle attack” (wie funktioniert sie) und wie kann eine Abhilfe aussehen ? (2 Punkte)

44.) Erklären sie die Funktionsweise der Hash-Funktion MD-5. Entspricht diese dem State-of-the-Art ? Welche sichere Alternativen gibt es ? (2 Punkte)

45.) Beschreiben sie die Anwendungsbereiche, Funktionsweise, Funktionalitäten und insbesondere die beiden “Schichten” von SSL und TLS. (2 Punkte)

46.) Beschreiben sie die beiden wesentlichen Strategien zum Schlüsselmanagement im Bereich sichere E-mail und ordnen sie die besprochenen Systeme jeweils einer Strategie zu. (2 Punkte)

47.) Erklären sie die Grundfunktionalitäten von DNSSEC (was wird wie abgesichert, was nicht - im Gegensatz zu IPSec, welche zusätzlichen DNS records gibt es dafür) und beschreiben sie wie die Problematik der Überprüfung der Korrektheit eines public domain-keys gelöst wird. (2 Punkte)

48.) Erklären sie die Grundstruktur und Funktionsweise von AES (was ist das für ein cipher, welche funktionellen Grundkomponenten hat er und was tun diese) und diskutieren sie die Unterschiede (und deren Grund) zu DES. (2 Punkte)

49.) Beweisen sie die Korrektheit der RSA Entschlüsselung für den Fall dass der numerische Nachrichtenblock und der Modul relativ prim sind (unter Verwendung des “kleinen” Fermat). (2 Punkte)

50.) Leiten sie die folgende Formel für die Eulersche ϕ-Funktion her: $\phi(n) = (p-1)(q-1)$ für $n = pq$ und p, q prim. (2 Punkte)

51.) Beschreiben sie die in der VO besprochene Protokollattacke gegen (automatisierte) digitale Empfangsbestätigungen (verschlüsselt & signiert) und diskutieren sie deren Realitätsnähe. (2 Punkte)

52.) Erklären sie wie das Knapsack-Problem verwendet werden kann, um ein public-key Verschlüsselungsverfahren zu realisieren. Warum werden solche Systeme heute nicht mehr eingesetzt ? (2 Punkte)

53.) Benennen und erklären sie mindestens zwei weitere zentrale Aufgaben der Kryptographie neben der Entwicklung von Verschlüsselungsverfahren und geben sie je ein konkretes Beispiel von entwickelten Systemen die diese Aufgaben erledigen . (2 Punkte)

54.) Erklären sie den Unterschied zwischen Block- und Streamcipher und geben sie je ein Beispiel. (1 Punkt)

55.) Erklären sie, warum man XOR-Verschlüsselung mit einem kurzen Key (im Gegensatz zum one-time Pad) als polyalphabetischen Cipher interpretieren kann. Aus wievielen Alphabethen besteht dieser polyalphabetische Cipher ? Was nützten diese Erkenntnisse bei der Entschlüsselung eines Ciphertexts, der mit XOR-short key verschlüsselt wurde ? (2 Punkte)

56.) Berechnen sie für den Modul $p = 5$ eine digitale Signatur nach El Gamal für die Nachricht $M = 3$ nach entsprechender (korrekter) Wahl der zusätzlich dafür notwendigen Parameter und führen sie auch die Verifikation der Signatur durch. (2 Punkte)

57.) Erklären sie detailliert das Ausmass der Fehlerausbreitung und warum es zu self-recovery kommt bei den CFB and CTR Blockcipher Betriebsmodi im Fall eines vorliegenden Ciphertext Bitfehlers. (2 Punkte)

58.) Rechnen sie exemplarisch zwei Iterationen des Feige-Fiat Shamir Identification Schemas durch: $p = 2$, $q = 3$, $s = 5$; eine Iteration mit der Challenge $b = 0$, die andere mit $b = 1$. Führen sie alle notwendigen Überprüfungen und Parameterwahlen durch und erklären sie warum trotz der übermittelten Daten durch Peggy die zero-knowledge Eigenschaft erhalten bleibt. (2 Punkte)

59.) Berechnen sie für den Modul $p = 5$ den Ciphertext nach El Gamal Verschlüsselung für die Nachricht $M = 3$ nach entsprechender (korrekter) Wahl der zusätzlich dafür notwendigen Parameter. Führen sie auch die Entschlüsselung durch und erklären sie, was ein Angreifer bei einer Ciphertext only Attacke können müsste um den Plaintext zu gewinnen (wir nehmen an dass der Angreifer den Parameter K für die randomisierte Verschlüsselung erhalten hat). (2 Punkte)

60.) Beschreiben sie die besprochenen CBC triple encryption Varianten. Nennen sie zwei Gründe, warum sie eine der beiden bevorzugen würden. Diese Verfahren wurden für DES entwickelt - macht eine Anwendung mit AES ebenfalls Sinn ? Begründen sie ihre Antwort ! (2 Punkte)

61.) Erklären Sie die Grundidee der quantenkryptographischen Schlüsselerzeugung und warum es beim beschriebenen Verfahren möglich ist zu erkennen ob ein Lauscher am Kanal war (2 Punkte).

VIEL ERFOLG !!