Aufgaben

13.1. In dieser Aufgabe betrachten wir einige Varianten zur Schlüsselableitung. In der Praxis wird oft zunächst ein Hauptschlüssel k_{MK} ausgetauscht, beispielsweise mit einem DHKE mit Zertifikaten. Nachfolgend werden von dem Hauptschlüssel Sitzungsschlüssel abgeleitet. Hier sind drei Möglichkeiten:

(1) $k_0 = k_{MK}$; $k_{i+1} = k_i + 1$
(2) $k_0 = h(k_{MK})$; $k_{i+1} = h(k_i)$
(3) $k_0 = h(k_{MK})$; $k_{i+1} = h(k_{MK}||i||k_i)$

$h()$ ist eine sichere Hashfunktion ist und k_i der i-te Sitzungsschlüssel.

1. Was ist der Hauptunterschied zwischen den drei Methoden?
2. Welches Verfahren weist *perfekte Vorwärtssicherheit* auf?
3. Wir nehmen an, dass Oskar den n-ten Sitzungsschlüssel erhalten hat (z. B. durch eine zeitaufwendige vollständige Schlüsselsuche). Welche der Sitzungen kann er jetzt entschlüsseln?
4. Welche Methode ist auch dann noch einsetzbar, wenn der Hauptschlüssel k_{MK} kompromittiert wurde? Begründen Sie die Antwort.

13.2. Wir betrachten ein Netzwerk mit 1000 Teilnehmern, die jeweils paarweise sicher und authentisiert kommunizieren wollen. Es soll jedoch kein Schlüsselserver oder eine anderweitige vertrauenswürdige zentrale Instanz einsetzt werden.

1. Wie viele Schlüssel werden systemweit benötigt?
2. Wie viele Schlüssel braucht man, wenn nun doch ein Schlüsselserver eingesetzt wird?
3. Was ist der Hauptvorteil beim Einsatz eines Schlüsselservers?
4. Wie viele Schlüssel werden im System benötigt, wenn asymmetrische Algorithmen benutzt werden?

Unterscheiden Sie zwischen Schlüsseln, die jeder Teilnehmer speichern muss und solchen, die für alle Teilnehmer bestimmt sind.

13.3. Ihre Aufgabe ist es, das Kryptoverfahren für einen Schlüsselserver auszuwählen. Hierbei treten zwei Arten von Verschlüsselungen auf:

- $e_{k_{U,KDC}}()$, wobei U ein beliebiger Benutzer des Netzes ist;
- $e_{k_{ses}}()$ für die Verschlüsselung einer Sitzung zwischen zwei Teilnehmern.

Zur Wahl stehen zwei Algorithmen, DES und 3DES (Triple-DES), wobei für beiden Verschlüsselungsarten unterschiedliche Chiffren gewählt werden sollen. Welchen Algorithmus empfehlen Sie für welche Verschlüsselung? Begründen Sie Ihre Antwort.

13.4. In dieser Aufgabe betrachten wir die Sicherheit von Systemen, die auf Schlüsselservern basieren. Wir nehmen an, einem Angreifer ist es gelungen, zum Zeitpunkt t_x Zugriff auf den Schlüsselserver zu erhalten. Er hat dabei alle Schlüssel stehlen können. Weiterhin gehen wir davon aus, dass dieser Angriff bemerkt wurde.

1. Welche Maßnahmen sollten getroffen werden, damit der Angreifer zukünftige Kommunikation zwischen den Teilnehmern nicht entschlüsseln kann?
2. Was genau ist seitens des Angreifers notwendig, um Nachrichten, die zu einem früheren Zeitpunkt t, wobei $t < t_x$, ausgetauscht wurden, zu dechiffrieren? Weist das System die Eigenschaft der perfekten Vorwärtssicherheit auf?

13.5. In dieser Aufgabe wird eine verbesserte Version eines Schlüsselservers betrachtet. In dem System werden alle Schlüssel $e_{k_{U,KDC}}()$ relativ häufig durch neue ersetzt, wobei das folgende Protokoll genutzt wird:

- Der Schlüsselserver erzeugt neue zufällige Schlüssel $k_{U,KDC}^{(i+1)}$.
- Der Schlüsselserver sendet die neuen Schlüssel an Teilnehmer U, wobei der neue Schlüssel mittels des alten chiffriert wird:

$$e_{k_{U,KDC}^{(i)}}(k_{U,KDC}^{(i+1)})$$

Welche Nachrichten können entschlüsselt werden, wenn angenommen wird, dass ein Mitarbeiter des Betreibers des Schlüsselservers bestechlich ist und alle aktuellen Schlüssel $k_{U,KDC}^{(i)}$ an einen Angreifer zum Zeitpunkt t_x verkauft? Diese Schlüsselpreisgabe wird erst wesentlich später zum Zeitpunkt t_y entdeckt, z. B. erst nach einem Jahr.

13.6. Zeigen Sie einen Schlüssel-Bestätigungsangriff gegen das Protokoll mit Schlüsselserver aus dem Unterkapitel 13.2.1. Beschreiben Sie alle Schritte des Angriffs mit Hilfe einer Skizze. Lehnen Sie sich hierbei an den Schlüssel-Bestätigungsangriff gegen das zweite modifizierte Protokoll mit Schlüsselserver an.

13.7. Zeigen Sie, dass das vereinfachte Kerberos-Protokoll keine perfekte Vorwärtssicherheit aufweist. Zeigen Sie, wie Oskar alte und zukünftige Nachrichten entschlüsseln kann, wenn:

1. Alice' KEK k_A kompromittiert wird,
2. Bobs KEK k_B kompromittiert wird.

13.8. Erweitern Sie das Kerberos-Protokoll derart, dass sich Alice und Bob gegenseitig authentisieren. Begründen Sie, warum das Protokoll sicher ist.

13.9. Ihre Kollegen bei Ihrem neuen Arbeitgeber sind beeindruckt, dass Sie es geschafft haben, sich durch dieses Buch zu kämpfen. Ihre erste Aufgabe ist es, ein Pay-TV-System zu entwerfen, bei dem das Dechiffrieren von verschlüsselten Programmen nicht möglich sein soll. Für den Schlüsselaustausch wird das Diffe-Hellman-Protokoll mit sicheren Parametern, z. B. einem Modul mit 2048 Bit, verwendet. Aus Kostengründen steht in den Set-Top-Boxen beim Kunden allerdings nur DES zur Verfügung. Sie schlagen das folgende Verfahren zur Schlüsselableitung vor:

$$K^{(i)} = f(K_{AB} \parallel i), \tag{13.1}$$

wobei f eine Einwegfunktion ist.

1. Zunächst überlegen wir uns, ob ein Angreifer einen vollständigen Film mit akzeptablem Aufwand speichern kann. Wir nehmen eine Datenrate von 1 MBit/s an und eine Länge von 120 Minuten für einen Film. Wie viel Speicherplatz in GB (d. h. Gigabyte, wobei 1 M = 10^6 und 1 G = 10^9) wird für das Abspeichern eines zweistündigen Films benötigt? Kann diese Datenmenge kostengünstig gespeichert werden?
2. Die Annahme ist nun, dass ein Angreifer einen DES-Schlüssel mittels vollständiger Schlüsselsuche innerhalb von 10 Minuten finden kann. Trotz der kurzen Schlüssellänge von DES ist dies immer noch eine sehr optimistische Annahme für den Angreifer, aber wir erreichen damit, dass das System auch noch mittelfristig sicher bleibt, da die Schlüsselsuche zunehmend einfacher wird. Wie häufig muss ein neuer Schlüssel abgeleitet werden, wenn wir erreichen wollen, dass die Dechiffrierung eines einzelnen Films mindestens 30 Tage dauern soll?

13.10. Gegeben sei ein Schlüsselaustausch nach Diffie-Hellman, bei dem der Schlüssel k_{AB} berechnet wird. Weitere Sitzungsschlüssel werden von k_{AB} nach dem folgenden Verfahren abgeleitet:

$$k^{(i)} = h(k_{AB} \parallel i), \tag{13.2}$$

wobei i eine Zählervariable ist, beispielsweise eine Ganzzahl mit 32 Bit. Der Wert von i ist öffentlich, er wird z. B. im Kopf einer jeden verschlüsselten Nachricht im Klartext mit übertragen. Für die eigentliche Verschlüsselung der Nutzdaten werden die abgeleiteten Schlüssel $k^{(i)}$ verwendet. Wir nehmen an, dass ein neuer Sitzungsschlüssel alle 60 Sekunden erzeugt wird.

1. Wir nehmen an, dass der Diffie-Hellman-Schlüsselaustausch einen Primzahlmodul mit der relativ kurzen Länge von 512 Bit verwendet und die Datenverschlüsselung mit AES erfolgt. Warum ist die oben stehende Schlüsselableitung in diesem Fall kryptografisch nicht sehr sinnvoll? Beschreiben Sie einen Angriff gegen das System, der möglichst effizient ist.
2. Wir nehmen jetzt an, dass der Schlüsselaustausch nach Diffie-Hellman mit einem 2048-Bit-Modul durchgeführt wird und für die Datenverschlüsselung DES eingesetzt wird. Beschreiben Sie den Vorteil, den diese Schlüsselableitung im Vergleich zu einer Lösung bietet, bei der nur ein DES-Schlüssel aus dem Diffie-Hellman-Protokoll berechnet wird.

13.11. Wir betrachten den Schlüsselaustausch nach Diffie-Hellman. Oskar führt hierbei den in Abschnitt 13.3.1 beschriebenen Mann-in-der-Mitte-Angriff durch. Wir nehmen an, dass für den Schlüsselaustausch die Parameter $p = 467$, $\alpha = 2$, $a = 228$ (für Alice) und $b = 57$ (für Bob) verwendet werden. Oskar verwendet den Wert $o = 16$. Berechnen Sie die Schlüssel k_{AO} und k_{BO} auf zwei Arten: (i) so, wie sie von Oskar berechnet werden, und (ii) so, wie sie von Alice bzw. Bob berechnet werden.

13.12. In dieser Aufgabe wird der Diffie-Hellman-Schlüsselaustausch mit Zertifikaten betrachtet. Es gibt die drei Teilnehmer Alice, Bob und Charley. Die Diffie-Hellman-Parameter sind $p = 61$ und $\alpha = 18$. Die privaten Schlüssel der drei Teil-

nehmer sind $a = 11$, $b = 22$ und $c = 33$. Die Seriennummern, mit denen die Teilnehmer sich identifizieren, sind $\mathrm{ID}(A) = 1$, $\mathrm{ID}(B) = 2$ und $\mathrm{ID}(C) = 3$. Es wird das Signaturverfahren von Elgamal mit den Parametern $p' = 467$, $d' = 127$, $\alpha' = 2$ und β verwendet. Die Zertifizierungsstelle (CA) verwendet die temporären Schlüssel $k_E = 213$ (für Alice), $k_E = 215$ (für Bob) und $k_E = 217$ (für Charley). (Bemerkung: In der Praxis sollte die CA einen besseren Zufallszahlengenerator einsetzen, um die Schlüssel k_E zu erzeugen.) Für die Zertifikate berechnet die CA $x_i = 4 \times b_i + \mathrm{ID}(i)$ und nimmt diesen Wert als Eingang für den Signaturalgorithmus. (Aus einem gegebenen Wert x_i lässt sich die $\mathrm{ID}(i)$ dann über $\mathrm{ID}(i) \equiv x_i \bmod 4$ berechnen.)

1. Berechnen Sie die drei Zertifikate $Cert_A$, $Cert_B$ und $Cert_C$.
2. Verifizieren Sie alle drei Zertifikate.
3. Berechnen Sie die drei Sitzungsschlüssel k_{AB}, k_{AC} sowie k_{BC}.

13.13. Oskar versucht einen aktiven Substitutionsangriff gegen den Diffie-Hellman-Schlüsselaustausch mit Zertifikaten. Er geht dabei wie folgt vor:

1. Alice möchte mit Bob kommunizieren. Wenn Alice das Zertifikat C(B) von Bob erhält, ersetzt Oskar dieses mit dem (gültigen!) Zertifikat C(O). Wie wird dieser Angriff entdeckt werden?
2. Bei einem weiteren Angriff, den Oskar versucht, ersetzt er Bobs öffentlichen Schlüssel b_B mit seinem eigenen Schlüssel b_O. Warum wird auch dieser Angriff bemerkt werden?

13.14. In dieser Aufgabe wird das Protokoll zur Zertifikatsausstellung mit CA-generierten Schlüsseln betrachtet. Es wird angenommen, dass die zweite Nachricht $(\mathrm{Cert}_A, k_{pr,A})$ über einen authentisierten Kanal übertragen wird, der aber nicht vertraulich ist, d. h. Oskar kann die Nachricht mitlesen.

1. Zeigen Sie, wie Oskar Nachrichten entschlüsseln kann, die mit einem Schlüssel chiffriert wurden, welchen Alice und Bob mittels des Diffie-Hellman-Protokolls erzeugt haben.
2. Kann Oskar sich auch gegenüber Bob als Alice ausgeben, d. h. kann er mit Bob einen Diffie-Hellman-Schlüsselaustausch vornehmen, ohne dass Bob es bemerkt?

13.15. Gegeben sei ein System, bei dem sich alle Teilnehmer die Diffie-Hellman-Parameter α und p teilen. Alle öffentlichen Schlüssel der Teilnehmer wurden durch eine CA zertifiziert. Wenn zwei Nutzer vertraulich kommunizieren möchten, führen sie einen Diffie-Hellman Schlüsselaustausch durch, bei welchem sie einen Sitzungsschlüssel erzeugen, den sie beispielsweise für AES verwenden können.

Wir nehmen an, dass Oskar in den Besitz des privaten Schlüssels der CA kommt, mit dem die Zertifikate generiert wurden. Kann er nun Nachrichten entschlüsseln, die Teilnehmer ausgetauscht haben, bevor er in den Besitz des privaten CA-Schlüssels gekommen ist? Begründen Sie Ihre Antwort.

13.16. Ein Problem bei Zertifikatssystemen ist die authentisierte Übertragung des öffentlichen Schlüssels der CA, mit dem die Zertifikate verifiziert werden. Wir nehmen an, dass Oskar vollständige Kontrolle über Bobs Kommunikationskanal hat,

d. h. er kann alle Nachrichten von und zu Bob beliebig verändern. Oskar ersetzt nun den öffentlichen CA-Schlüssel durch seinen eigenen Schlüssel. (Man beachte, dass Bob keine Möglichkeit hat, die Echtheit diese Schlüssels zu überprüfen, so dass er annimmt, dass es sich um den CA-Schlüssel handelt.)

1. (Zertifikatsausstellung) Bob möchte nun ein Zertifikat bei der CA anfordern. Er sendet dafür eine Nachricht, die (1) seine Identität $ID(B)$ und (2) seinen öffentlichen Schlüssel B enthält. Welche Schritte muss Oskar unternehmen, so dass Bob nicht bemerkt, dass er nicht im Besitz des CA-Schlüssels ist?
2. (Protokollausführung) Beschreiben Sie, wie Oskar mit Bob einen authentisierten Diffie-Hellman-Schlüsselaustausch durchführen kann. Bob soll hierbei nicht bemerken, dass er nicht mit Alice kommuniziert.

13.17. Zeigen Sie den Ablauf eines Protokolls zum Schlüsseltransport, bei dem der RSA-Algorithmus eingesetzt wird. Lehnen Sie sich hierzu an Abbildung 6.5 in Abschnitt 6.1 an.

13.18. In dieser Aufgabe betrachten wir RSA mit Zertifikaten. Bob ist im Besitz eines öffentlichen und eines privaten RSA-Schlüssels. Oskar gelingt es, Alice einen gefälschten CA-Schlüssel $k_{pub,CA}$ zuzusenden, für den er den passenden privaten Schlüssel hat. Entwickeln Sie einen aktiven Angriff, bei dem Oskar Nachrichten dechiffrieren kann, die Alice an Bob sendet. Muss Oskar hierfür einen Mann-in-der-Mitte-Angriff durchführen?

13.19. Pretty Good Privacy (PGP) ist ein weit verbreitetes Programm, mit welchem E-Mails verschlüsselt und signiert werden können. PGP erfordert keine Zertifikate. Beschreiben Sie das Vertrauensmodell von PGP und die Funktionsweise der PGP-Schlüsselverteilung.