Klausur Grundlagen IT-Sicherheit und Kryptographie

Salzburg, T02, 14:15 *16.11.2007*

1.) Zum Verständnis von RSA: gegeben sind als public key $n = 15$ und $e = 7$. Sie fangen einen Ciphertext $c = 8$ ab. Ermitteln Sie durch eine Faktorisierungs-Attacke den dazugehörigen Plaintext und erklären Sie die Rolle der Faktorisierung bei Ihrer Attacke. (2 Punkte)

2.) Erklären Sie die Betriebsarten von Blockciphern (ECM, CBC, CFB, OFB) und deren Vor- und Nachteile. (2 Punkte)

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

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

5.) Wie können symmetrische Block-cipher verwendet werden um one-way Hash functions daraus bauen zu können ? Erklären Sie das anhand des Davies-Mayer Algorithmus. (2 Punkte)

6.) 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)

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

8.) Wie funktioniert das SKEY Authentifizierungssystem ? (1 Punkt)

VIEL ERFOLG !!

1) Zum Verständnis von RSA: gegeben sind als public key n=15 und e=7.
   Ver- und entschlüsseln sie die Nachricht M=8 mittels RSA.

2) Wie könnte eine Mischung zwischen public key und symmetrischen Verfahren funktionieren (Stichwort: Hybride Verfahren). Warum ist so ein Verfahren sinnvoll?

3) Wie funktioniert die Geburtstagsattacke gegen one-way Hash funktionen. Worauf beruht sie?

4) Was ist die „meet in the middle attack“ und was sind die Konsequenzen ihres Daseins?

5) Erklären Sie die Grundprinzipien von elliptic curve cryptography, die Vor.+- und Nachteile, und die Anwendungsbereiche für die diese Verfahren besonders interessant sind.

6) Erklären Sie anhand eines einfachen Protokolls den Diffie-Hellman Key-exchange Algorithmus. Wählen Sie n=5 und rechnen Sie ein konkretes Beispiel durch.

7) Eas ist ein Zero-Knowledge Protokoll und was ist der Unterschied zu z.B. klassischen Authentifizierungsprotokollen? Beschreiben Sie detailliert die Funktionsweise des Feige-Fiat Schamit Identifikations Schemas und erklären Sie die zero-knowledge Eigenschaft.

8) Wie funktionert SKEY?

Klausur Grundlagen IT-Sicherheit und Kryptographie

Salzburg *29.7.2005*

1.) Zum Verständnis von RSA: gegeben sind als public key $n = 15$ und $e = 7$. Sie fangen einen Ciphertext $c = 8$ ab. Ermitteln Sie durch eine Attacke den dazugehörigen Plaintext und erklären Sie die Rolle der Faktorisierung bei Ihrer Attacke. (2 Punkte)

2.) Erklären Sie die Betriebsarten von Blockciphern (ECM, CBC, CFB, OFB) und deren Vor- und Nachteile sowie die Fehlerausbreitung. (2 Punkte)

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

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

5.) Erklären Sie die wesentlichen Bestandteile eines Kerberos Realms und den Ablauf einer Applikationsanforderung und Durchführung. Was sind Nachteile von Kerberos ? (2 Punkte)

6.) Was ist die "man in the middle attack" und wie kann eine Abhilfe aussehen ? (2 Punkte)

7.) 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. (2 Punkte)

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

VIEL ERFOLG !!

TEST zur VL: Grundlagen der IT-Sicherheit und Kryptographie 4. 7. 2002

1. Was ist die „meet in the middle attack“ und wie kann die nicht-Gruppenstruktur von DES sonst ausgenutzt werden? (2 Punkte)

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

3. Erklären Sie Betriebsarten von Blockciphern (ECM, CBC, CFB, OFB) und diskutieren Sie jeweils kurz die Errorpropagation. (3 Punkte)

4. Erklären Sie die Funktionsweise von RSA und die mathematische Grundlage der Entschlüsselung (im einfachen Fall (mi, n) = 1). Wo geht „Euler“ ein? (2 Punkte)

5. Erklären Sie anhand eines einfachen Protokolls den Diffie-Hellman Key-exchange Algorithmus. Wählen Sie n = 7 und rechnen Sie ein konkretes Beispiel durch. (2 Punkte)

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

7. Welcher Zahl im Restklassensystem Modulo 11 entspricht der Ausdruch – 5/4 (mod 11)? Erklären Sie die Berechnungsschritte. (2 Punkte)

8. Wie können symmetrische Block-cipher verwendet werden um one-way Hash functions daraus bauen zu können? Erklären Sie das anhand der Verwendung von AES für so ein System (was ist Key, was ist Input, was ist der Hashwert, jeweilige Länge der Komponenten, ...). (2 Punkte)

9. Welches Problem wird bei SET durch sog. Duale Signaturen gelöst und wie funktioniert das? (2 Punkte)

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

TEST zur VL: Kryptographie *3.2.1999*

Anmerkung des Scanners: Zeit gab es so viel wie benötigt, i.e. open end

1.) Was ist die "man in the middle attack" und wie kann eine Abhilfe aussehen ?

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

3.) Erklären Sie Betriebsarten von Blockciphern (ECM, CBC, CFB, OFB) und diskutieren Sie jeweils kurz die Errorpropagation.

4.) Erklären Sie die Funktionsweise von RSA und die mathematische Grundlage der Entschlüsselung (im einfachen Fall $(m_i, n) = 1$). Wo geht "Euler" ein ?

5.) Erklären Sie anhand eines einfachen Protokolls den Diffie-Hellman Key-exchange Algorithmus.

6.) Wie funktioniert die Geburtstagsattacke gegen one-way Hash functions ? Worauf beruht sie ? Abhilfe ?

7.) Wie funktioniert der Merkle-Hellman Algorithmus ?

8.) Wie können symmetrische Block-cipher verwendet werden um one-way Hash functions daraus bauen zu können ? Erklären Sie das anhand des Tandem Davies-Mayer Algorithmus.

9.) Was ist die "common modulus attack" gegen RSA, wie funktioniert sie, wie kann Abhilfe geschaffen werden ?

10.) Erklären Sie die Funktionsweise (und deren mathematische Grundlage) von Digitalen Signaturen mittels El Gamal Algorithmus.