Computer and network security. Final exam 14-06-2012. Time: 120 minutes

1. Diffie-Hellman

With reference to Diffie-Hellman key exchanging scheme, answer:

- How is the key computed and what are the requirements on the numbers used for such a computation?
- Try generalizing the DH scheme for exchanging a key among three subjects.
- Discuss the robustness of DH wrt active attacks and possible countermeasures.

2. Access control models

- Illustrate the DAC model (from Harrison-Ruzzo-Ullman, or HRU), define the concept of safety of the protection system and discuss what practical problems arise within the model.
- Why such DAC model is vulnerable to Trojans? What type of access control model can prevent them from illegally access private data? Discuss.

3. Message authentications codes (MACs)

Briefly define purposes of data integrity and authentication. Then answer:

- Alice wants to send a file F to Bob, ensuring integrity and confidentiality; they share a symmetric key KAB and can use AES (no hashing function is available). Alice sends to Bob: $Enc_{KAB}(F)$. Are integrity and confidentiality guaranteed? Discuss.
- Enrich the communication schema for better fulfilling integrity and confidentiality.

4. RSA

- Describe the encrypting/decrypting scheme of pure RSA. Describe at least two vulnerabilities of pure RSA. Also discuss how real implementations of RSA contrast such vulnerabilities.
- Discuss the following use of RSA for confidentiality: Alice sends to Bob $Enc_{KPubB}(F)$. Is confidentiality guaranteed? Can you illustrate any variant, still RSA-based, but also using symmetric cryptography (no pre-shared symmetric keys available) and lowering CPU time?

5. Briefly answer the following (at most 8 lines & 1 picture per question – using more space does not increase the quality)

- With reference to IPSec, define one or more security associations for securing the following scenario: Alice is using her home PC and wants to print a document stored in her PC on the company printer.
- Consider using the bits of a zipped file for implementing a pseudo-random number generator (PRNG). Discuss the quality of this PRNG for cryptographic purposes.

Sicurezza nelle reti e nei sistemi informatici. Esame del 14-06-2012. Tempo: 120 minuti

1. Diffie-Hellman

Con riferimento allo schema di scambio chiavi di Diffie-Hellman, rispondere:

- Come viene calcolata la chiave e quali sono I requisiti dei numeri utilizzati?
- Generalizzare lo schema DH per lo scambio di una chiave fra tre soggetti.
- Discutere la robustezza di DH rispetto ad attaccanti attivi e le possibili contromisure.

2. Modelli per il controllo degli accessi
Access control models

- Illustrare il modello DAC (da Harrison-Ruzzo-Ullman, o HRU), definire il concetto di safety del sistema di protezione e discutere quali problemi pratici intervengono nel modello.
- Perché tale modello DAC è vulnerabile ai Trojan? Che tipo di modello per il controllo degli accessi può prevenire il loro accesso illegittimo ai dati provati? Discutere.

3. Message authentications codes (MACs)

Definire brevemente gli obiettivi dell'autenticazione e dell'integrità dei dati. Quindi rispondere:

- Alice vuole inviare il file F a Bob, garantendo integrità e confidenzialità. I due condividono una chiave simmetrica KAB e possono utilizzare AES (ma non sono disponibili funzioni di hashing). Alice invia a Bob: $Enc_{KAB}(F)$. Ciò garantisce gli obiettivi di integrità e confidenzialità? Discutere.
- Aumentare lo schema di comunicazione precedente ai fini di un più efficace conseguimento degli obiettivi di confidenzialità e integrità.

4. RSA

- Descrivere gli schemi di cifratura/decifratura dell'RSA puro. Descrivere almeno due vulnerabilità dell'RSA puro. Illustrare infine come le reali implementazioni di RSA consentono di contrastare tali vulnerabilità.
- Discutere il seguente uso di RSA ai fini della confidenzialità: Alice invia a Bob $Enc_{KPubB}(F)$. Ciò garantisce la confidenzialità? Illustrare una variante, ancora basata su RSA, ma che utilizza anche la crittografia simmetrica (non sono disponibili chiavi simmetriche precedentemente stabilite), che consente di ridurre gli oneri computazionali.

5. Rispondere brevemente alle seguenti domande (max 8 linee e una figura per domanda – l'utilizzo di spazio aggiuntivo non migliora la risposta)

- Con riferimento a IPSec, definire una o più associazioni di sicurezza adatte a mettere in sicurezza il seguente scenario: mentre è a casa usando il proprio pc, Alice desidera stampare un documento locale sulla stampante aziendale.
- Esaminare la possibilità di utilizzare I bit di un file zippato per realizzare un generatore di numeri pseudo-casuali (PRNG). Discutere la qualità di un tale PRNG ai fini crittografici.