*Contrairement à l'usage plusieurs questions de cet examen sont des questions ouvertes qui admettent plusieurs réponses. Vous devez justifier le choix de vos réponses et détailler les hypothèses que vous adoptez. Vous devez aussi choisir la précision et la longueur de vos réponses pour respecter le temps limité (deux heures) et pour traiter toutes les questions de manière équilibrée.*

**Exercice 1.** Dans la RFC 2401 « Security architecture for the internet protocole » on trouve le paragraphe suivant :

> The suite of IPsec protocols and associated default algorithms are designed to provide high quality security for Internet traffic. However, the security offered by use of these protocols ultimately depends on the quality of the their implementation, which is outside the scope of this set of standards. Moreover, the security of a computer system or network is a function of many factors, including personnel, physical, procedural, compromising emanations, and computer security practices. Thus IPsec is only one part of an overall system security architecture.

**1.** Discuter les relations entre cryptographie et sécurité.

**2.** Quelles tailles de clé AES et RSA vous semblent garantir une confidentialité raisonnable ?

**3.** Le groupement des cartes bancaires utilisait jusqu'en 1998 pour l'authentification des cartes à puces une clé RSA de 320 bits. Combien de temps faut-il pour casser une telle clé ?

**4.** Expliquer le schéma de signature RSA (expliquer en particulier pourquoi on utilise une fonction de hachage)

**Exercice 2.** Dans la même RFC 2401 on trouve :

3.3 Where IPsec May Be Implemented

> There are several ways in which IPsec may be implemented in a host or in conjunction with a router or firewall (to create a security gateway). Several common examples are provided below:
>
> a. Integration of IPsec into the native IP implementation. [...]
>
> b. "Bump-in-the-stack" (BITS) implementations, where IPsec is implemented "underneath" an existing implementation of an IP protocol stack, between the native IP and the local network drivers. [...] This approach, when it is adopted, is usually employed in hosts.
>
> c. The use of an outboard crypto processor is a common design feature of network security systems used by the military, and of some commercial systems as well. It is sometimes referred to as a "Bump-in-the-wire" (BITW) implementation. Such implementations may be designed to serve either a host or a gateway (or both). Usually the BITW device is IP addressable. When supporting a single host, it may be quite analogous to a BITS implementation, but in supporting a

```
router or firewall, it must operate like a security gateway.
```

**1.** Discuter les interférences entre le routage IP et IPsec. Dans quel ordre doivent-ils intervenir ?

**2.** Décrire le traitement (routage et IPsec) d'un paquet sortant.

**Exercice 3.** **1.** Expliquer pourquoi le chiffrement à masque jetable est parfaitement sûr (on pourra faire une démonstration mathématique utilisant les probabilités).

**2.** Décrire une attaque contre le chiffrement par bloc en mode ECB (*Electronic Code Book*) lorsqu'il est utilisé lors d'une connexion SSH (c'est à dire avec une contrainte de délai très court et un débit très bas). On montrera que cette attaque ne dépend pas de la qualité de l'algorithme de chiffrement utilisé.

**3.** Expliquer pourquoi l'utilisation du mode CBC (*Cipher block chaining*) protège une telle connexion.

**4.** Pourquoi une utilisation naïve (c'est-à-dire sans utilisation de vecteur initial) du mode CBC ne protège pas contre une telle attaque lors de l'utilisation d'ESP-IPSec sur une connexion avec les mêmes caractéristiques (délai court et bas débit)

**5.** On trouve en effet dans la RFC 2406 « IP-ESP » :

```
If the algorithm used to encrypt the payload requires cryptographic
synchronization data, e.g., an Initialization Vector (IV), then this
data MAY be carried explicitly in the Payload field.  If such
synchronization data is implicit, the algorithm for deriving the data
MUST be part of the RFC.
```

Et dans la RFC 3602 « The AES-CBC Cipher Algorithm and Its Use with IPsec »

```
This document specifies the use of the AES cipher in CBC
mode within ESP.  This mode requires an Initialization Vector (IV)
that is the same size as the block size.  Use of a randomly generated
IV prevents generation of identical ciphertext from packets which
have identical data that spans the first block of the cipher
algorithm's block size.

The IV is XOR'd with the first plaintext block before it is
encrypted.  Then for successive blocks, the previous ciphertext block
is XOR'd with the current plaintext, before it is encrypted.
```

Et un peu plus loin dans la même RFC :

```
3.  ESP Payload

   The ESP payload is made up of the IV followed by raw cipher-text.
   Thus the payload field, as defined in [ESP], is broken down according
   to the following diagram:

   +---------------+---------------+---------------+---------------+
   |                                                               |
   +               Initialization Vector (16 octets)               +
   |                                                               |
   +---------------+---------------+---------------+---------------+
   |                                                               |
   ~ Encrypted Payload (variable length, a multiple of 16 octets)  ~
```

```
|                                                               |
+---------------------------------------------------------------+
```

```
The IV field MUST be the same size as the block size of the cipher
algorithm being used.  The IV MUST be chosen at random, and MUST be
unpredictable.

Including the IV in each datagram ensures that decryption of each
received datagram can be performed, even when some datagrams are
dropped, or datagrams are re-ordered in transit.

To avoid CBC encryption of very similar plaintext blocks in different
packets, implementations MUST NOT use a counter or other low-Hamming
distance source for IVs.
```

À la lecture de cette documentation expliquer comment IPsec se protège de l'analyse de trafic. Quelles doivent être les propriétés du générateur aléatoire d'IV ? Quelles sont néanmoins les informations que l'ont peut obtenir par analyse du trafic IPsec ?