Se proponen los siguientes temas (notar que la lista puede ser ampliada más tarde si hace falta).

1. Criptografía simétrica (del 26 de octubre al 5 de noviembre)
   - *a*) La maquina Enigma.
   - *b*) El sistema DES (descripción y posibles ataques)
   - *c*) El sistema AES (descripción y posibles ataques)
   - *d*) Funciones de resumen (hash)
2. Criptografía asimétrica (del 9 de noviembre al 19 de noviembre)
   - *a*) Dinero digital
   - *b*) Protocolos de firma digital.
   - *c*) Otros protocolos basados en criptografía asimétrica.
   - *d*) Cifrado ElGamal (descripción y posibles ataques)
   - *e*) Criptosistemas basados en el problema de mochila (descripción y posibles ataques)
3. Primalidad y factorización (del 23 de noviembre al 3 de diciembre)
   - *a*) Símbolos de Jacobi. Pseudoprimos de Euler. Primos de Fermat.
   - *b*) El test de Lucas-Lehmer para los primos de Mersenne.
   - *c*) Test de primalidad AKS.
   - *d*) Los métodos de factorización de Pollard.
   - *e*) La criba cuadrática.
   - *f*) Ataques contra RSA.
4. Códigos Detectores/Correctores (del 14 de diciembre al 13 de enero)
   - *a*) Códigos de Huffman.
   - *b*) Códigos de Golay.
   - *c*) El teorema de Shanon.
   - *d*) Diseños y códigos.

El tema tiene que ser expuesto en clase y después hay que presentar un trabajo escrito (con más detalle). Para obtener una buena nota:

1. Hay que presentar el trabajo en fechas acordadas.
2. Tener por lo menos una primera versión del trabajo escrito antes de exponer el tema en clase.
3. Es obligatoro hacer una pequeña presentación del trabajo ante el profesor por lo menos 3 días antes de la charla en clase.
4. Se recomienda hacer trabajos escritos en Tex o Latex.
5. No olvidar poner la bibliografía consultada en los trabajos (incluida la de internet).