**復習用問題**

**１．社会的に価値のある暗号の使用方法を少なくとも３つ挙げて説明せよ。（どしてそれらが社会的に価値があるのか、についても触れよ。）**

**２．公開鍵暗号法と秘密鍵暗号法の決定的な違いは何か？**

**３．公開鍵暗号法をどのように用いると書類にデジタル”署名”をほどこすことができるのか、その仕組みを説明せよ。**

**４．第２次世界大戦中に政府によって禁止された通信はどのようなものであったか？**

**５．１９９４年の**(the Communications Assistance for Law Enforcement Act )**と、それ以前に政府が保持していた盗聴能力の主な違いは何か？**

**６．過去に犯罪者によって暗号が用いられた例を挙げよ。**

**７．暗号鍵を委託する際にプライベートなシステムを産業界が選択するであろう理由をいくつかあげよ。**

**一般問題**

**８．我々を守るために**(the Communications Assistance for Law Enforcement Act )**と、暗号鍵の強制的な委託制度が考え出された背景にあった脅威の中でも、特に 深刻だったと思うものを２つ挙げよ。**( the Communications Assistance for Law Enforcement Act )**に対する反対意見の中で特に強力だったと思うものを２つ挙げよ。さらに、暗号鍵の強制的な委託制度に対する反対意見の中で特に強力だったと思うものを２つ挙げよ。**

**９．本文中で挙げられていたＰＧＰの使用例は、（１）ネオナチが違法行為を行うための情報を書き込む掲示板、（２）恐らく第３世界においては政府の認可を受けているであろう、暗殺集団の犠牲者や目撃者との情報送信、の２つである。では、政府が鍵を保管するべきかどうか、ということを考えたときに、これら２つの例は互いに均衡が保たれているであろうか？それとも、両者のうちの一方の ケースが一方の側により必然的な意見を導くだろうか？**

１０．（ａ）強力な暗号システムの輸出を制限することで、どうしてアメリカ人がアメリカ国内で強力な暗号を用いることがより困難かつコストがかかるようになるのか？
（ｂ）米国の暗号政策についての評論家の中には「政府が輸出制限を続けるのは米国民が強力な暗号を使用する機会を減らすためだ」と考える人もいる。政府の動きをこのように解釈するための、あるいは解釈しないための証拠は何か？
（ｃ）暗号ソフトやハードウェアの輸出について、制限をかけるのであればどのような制限をかけるべきなのか、あるいはかけないでよいのか？理由と共に述べよ。

１１．デジタルキャッシュは、安全かつ匿名性を保ってやりとりができるようにデザインされている。プライバシーにとってのプラスの面と、税金逃れや犯罪に使われるかもしれないと言うマイナスの面との両方を考えるとき、完全に匿名なデジタルキャッシュの使用は禁止されるべきだとあなたは考えるか？理由と共に述べよ。

１２．3.3.3節で挙げた商用鍵委託を思い出そう。政府のライセンスを持った鍵委託会社にすべてのユーザーが鍵を委託しないといけない、と法律で定めることについて賛成意見を述べよ。また、そのような要求について反論せよ。

**宿題**

*ここに挙げた問題を解くためにはちょっとしたリサーチが必要なので、 ビジネスアワー中に解いてもらうとか、もしくは宿題にするなら提出期限前に何日かの期間をもうける必要がある。*

１３．１９９４年制定の(the Communications Assistance for Law Enforcement Act ) の文面のコピーを手に入れた上で、以下の問に答えよ。（その際には訳のわからない法律用語を使うのではなく、自分の言葉を使って答えよ。）
（ａ）第１０３項がこの法律の最もメインの部分である。この項のパート（ａ）が述べている要求、およびパート（ｂ）が挙げている制限を要約せよ。
（ｂ）”テレコミュニケーション・キャリア” とは何を意味するか？
（第１０２項の定義を見よ。）
（ｃ）警察機関によって傍受された通信が暗号化されているとき、”テレコミュニケーション・キャリア”はどのような責任を負うか？
（ｄ）この法律の要求に従うと、”テレコミュニケーション・キャリア”の対応はどれぐらい早急でなければならないか？（第１０４項を見よ。）

**（ｅ）この法律は電話通信のスイッチング機器や伝達機器の製造者にどういった内容の要求やペナルティーを課すか？（第２０１項を見よ。）**

**１４．あなたの地域の警察署に連絡を取って、犯人の確証を取るために盗聴を行なうのはどのようなケースなのか、質問してみよう。そしてその要点を書き出せ 。**

**１５．インターネット上でＰＧＰのコピーを探せ。**

**１６．デジタルキャッシュ用のソフトウェアを製造している会社のWWWのホームページにアクセスして、その製品のうちの１つについてレポートせよ。その製品を使用する際の利点と欠点は何か？**

**１７．暗号政策に関するいくつかの法案は１９９６年に議会で導入された。その後、あるものはその適用を緩め、またあるものは適用がよりきつくなった。そのような法案の現在の状態を少なくとも１つ挙げよ。さらに、この本が出版されて以降、暗号に関する重要な立法がなされただろうか？**

**クラスで行なう練習**

**１．「すべての暗号鍵が委託されるべきだ」という法的な要求が必要かどうか、という問題についてクラスでディベートを行なえ。**