Solution to Moed Bet – Introduction to Cryptography 20580

Yehuda Lindell

January 26, 2006

Solution for question 1:

1. Fix a key k. Since every message in the key-space can be encrypted and decrypted with this key, we have that for every $x \neq x'$, $E_k(x) \neq E_k(x')$ (otherwise if $y = E_k(x') = E_k(x)$, decryption cannot always work). This implies that $|\mathcal{C}| \geq |\mathcal{P}|$.

2. Let $C(k) = \{e_k(x)\}_{x \in \mathcal{P}}$. Then, we know that

$$\Pr[\mathbf{y} = y] = \sum_{k: y \in C(k)} \Pr[\mathcal{K} = k] \Pr[\mathbf{x} = d_k(y)]$$

By Shannon's theorem for perfect secrecy, we know that $\Pr[\mathcal{K} = k] = 1/|\mathcal{K}|$ and that for every x and y there exists a single k such that $\mathbf{x} = d_k(y)$. In addition, we know that $C(k) = \mathcal{C}$. Therefore,

$$\Pr[\mathbf{y} = y] = \frac{1}{|\mathcal{K}|} \sum_{y \in \mathcal{C}} \Pr[\mathbf{x} = d_k(y)] = \frac{1}{|\mathcal{K}|} \sum_{y \in \mathcal{C}} \frac{1}{|\mathcal{K}|} = \frac{1}{|\mathcal{K}|}$$

where the last equality is due to the fact that $|\mathcal{C}| = |\mathcal{K}|$. Applying this fact again, we have that $\Pr[\mathbf{y} = y] = 1/|\mathcal{C}|$, as required.

Solution for Question 2:

1. The initial and final permutations IP and IP^{-1} have no effect on security because they do not involve the key and are known. This suffices, but a more formal answer states that if it is possible to break the scheme without IP then it is possible to feed DES with $IP^{-1}(x)$ and compute $IP(y)$ for the result. This has the effect of being equivalent to DES with the permutations removed.

2. If the permutation inside f is removed, the avalanche effect no longer exists. In particular, consider the encryption of two messages that differ only in the first bit. It holds that only 4 bits of the output will differ after encrypting these strings. This makes DES insecure because it is possible to detect repeating blocks, and in particular, DES does not behave in a random-like (pseudorandom) fashion.

Solution for Question 3: There is no problem to define RSA in this way. For key generation, choose 3 primes p, q, and r and compute $n = pqr$ and $\phi(n) = (p-1)(q-1)(r-1)$. Then, choose e that is relatively prime to $\phi(n)$ and $d = e^{-1} mod \phi(n)$. Encryption and decryption work as in RSA (I expect the students to show how).

Solution for Question 4:

1. The scheme remains secure. Intuitively, security follows from the fact that β^k is indistinguishable from a random string and so $\beta^k \cdot x$ works like a one-time pad. However, the same effect is achieved by $\beta^k + x$ (if β^k is random, then $\beta^k + x$ can also be any value in the field). Decryption is carried out by computing $x = y_2 - y_1^a = beta^k + x - \alpha^{ka} = x$.

2. Given two encryptions (y_1, y_2) and (y_1, y_2') of x and x' respectively, compute $y_2/y_2' mod p$. The result is $x/x' mod p$ which is open for a statistical attack. Decryption clearly remains the same.

3. Given $y_1 = \alpha^k$ and $y_2 = \beta^{kx}$ it follows that $y_2/y_1^a = \alpha^{ak-akx} = \alpha^{ak(1-x)}$. Solving this equation seems difficult.

Solution for Question 5:

1. A different third point will yield an incorrect secret because each different point defines a different polynomial with a different secret to be reconstructed.

2. The other two generals have no way of knowing which share is incorrect because every pair of points is consistent with every possible secret (by the proof that Shamir's secret-sharing is perfect).

3. Given a fourth general and a way of checking which secret is correct, each subset of 3 out of 4 general can reconstruct the secret and test if it is correct. Since the spy already revealed its incorrect share, this will be used in the computation and will yield an incorrect code.