THIS PAGE IS LEFT BLANK

BECAUSE Microsoft Word BUGS

WHEN TRANSLATING TO PostScript !

THIS PAGE IS LEFT BLANK

BECAUSE Microsoft Word BUGS

WHEN TRANSLATING TO PostScript !

THIS PAGE IS LEFT BLANK

BECAUSE Microsoft Word BUGS

WHEN TRANSLATING TO PostScript !

THIS PAGE IS LEFT BLANK

BECAUSE Microsoft Word BUGS

WHEN TRANSLATING TO PostScript !

CS547A Solution set #5

Exercises (from Stinson's book)

Exercise 6.1

(a) If we have the same γ for both, then $\beta^{\gamma}\gamma^{\delta_1} \equiv \alpha^{x_1} \pmod p$ and $\beta^{\gamma}\gamma^{\delta_2} \equiv \alpha^{x_2} \pmod p$ yield $\gamma^{\delta_2-\delta_1} \equiv \alpha^{x_2-x_1} \pmod p$ which leads to $k \equiv (x_2-x_1)(\delta_2-\delta_1)^{-1} \pmod{p-1}$ since $\gamma \equiv \alpha^k \pmod p$.

(b) When k is known solve $a\delta \equiv (x-k\gamma) \pmod{p-1}$ using either (x_1,δ_1) or (x_2,δ_2): $a\delta_k \equiv (x_k-\gamma(x_2-x_1)(\delta_2-\delta_1)^{-1}) \pmod{p-1}$ for $k\in\{1,2\}$.

(c) In this case, it is easier to use (x_2,δ_2) since gcd(20481,31846)=1 which means that δ_2^{-1} exists mod p-1. The answer is k = 1165 and a = 7459.

Exercise 6.3

Let p=467, α=2, β=132, x=100, γ=29, δ=51, h=102, i=45, j=293. So

$$\lambda = \gamma^h\alpha^i\beta^j \bmod p = 29^{102}\, 2^{45}\, 132^{293} \bmod 467 = 363$$

$$\mu = \delta\lambda(h\gamma-j\delta)^{-1} \bmod p-1 = 51*363(102*29-293*51)^{-1} \bmod 466 = 51*17 \bmod 466 = 401$$

$$x' = (hx+i\delta)\lambda(h\gamma-j\delta)^{-1} \bmod p-1 = (102*100+45*51)*17 \bmod 466 = 385$$

which leads to

$$\beta^{\lambda}\lambda^{\mu} \equiv 132^{363}\, 363^{401} \equiv 355 \equiv 2^{385} \equiv \alpha^{x'} \pmod p$$

Exercise 6.6

Let p=7879, q=101, α=170, β=4567, x=5001, k=49, a=75. So

$$\gamma = (\alpha^k \bmod p) \bmod q = (170^{49} \bmod 7879) \bmod 101 = 59$$

$$\delta = (x+a\gamma)k^{-1} \bmod q = (5001+75*59)49^{-1} \bmod 101 = 79$$

$$e_1 = x\,\delta^{-1} \bmod q = 5001*79^{-1} \bmod 101 = 16$$
$$e_2 = \gamma\,\delta^{-1} \bmod q = 59*79^{-1} \bmod 101 = 57$$

and finally

$$(\alpha^{e_1}\beta^{e_2} \bmod p) \bmod q = (170^{16}4567^{57} \bmod 7879) \bmod 101 = 59 = \gamma.$$

Exercise 7.5

Induction basis, i=1.

We assume h_1 is strongly collision-free.

Induction step, let i>1.

Assume for induction hypothesis (IH), that for any positive integer n<i we have that h_n is strongly collision-free.

Now assume we have found a collision (x,x') of h_i. By definition, we then have $h_i(x) = h_1(h_{i-1}(x_1)|| h_{i-1}(x_2)) = h_1(h_{i-1}(x'_1)|| h_{i-1}(x'_2)) = h_i(x')$. Since $x \neq x'$, there must exist a $k \in \{1,2\}$ such that $x_k \neq x'_k$. Two cases are then possible:

• either $h_{i-1}(x_k) \neq h_{i-1}(x'_k)$ in which case we have found a collision (y,y') of h_1, where $y = h_{i-1}(x_1)||h_{i-1}(x_2)$ and $y' = h_{i-1}(x'_1)||h_{i-1}(x'_2)$. This contradicts the IH.

• or $h_{i-1}(x_k) = h_{i-1}(x'_k)$ in which case we have found a collision (x_k,x'_k) of h_{i-1}. This also contradicts the IH.

Thus, if $h_1 \ldots h_{i-1}$ are strongly collision-free then h_i is also strongly collision-free.

Exercise 9.1

Suppose Bob picks r at random and sets $x \equiv r^2 \pmod n$. Now, let y be Alice's answer to query x. If ($r \neq y$ and $r \neq n-y$) then gcd(y-r,n) and gcd(y+r,n) are the prime factors p,q of n.

With the prime factors of n, Bob can computes square roots mod n (by computing square roots mod p and mod q) and identify as Alice…

Exercise 9.6

Let p=503, q=379, n=190637, b=509, u=155863, k=123845, r=487.

(a) $v = (u^{-1})^b \bmod n = (155863^{-1})^{509} \bmod 190637 = 128600$
(b) $\gamma = k^b \bmod n = (123845)^{509} \bmod 190637 = 162227$
(c) $y = ku^r \bmod n = 123845 * 155863^{487} \bmod 190637 = 51149$
(d) $\gamma = 162227 = 128600^{487} 51149^{509} \bmod 190637 = u^r y^b \bmod n$.

Other Exercises

(a) Show that $\pi_k(x,y)$ is indeed a permutation (a one-to-one function).

ANSWER:
follows from the existence of the inverse $\pi^{-1}_k(x,y)$ described in part (e).

(b) Show that $\{ \pi_k : \{0,1\}^{2n} \rightarrow \{0,1\}^{2n} \}_k$ is not a PRΠG.

ANSWER:
Indeed we show that it is not a PRΦG. Consider the following distinguisher T:

On input $[(x_1,y_1), (u_1,v_1)], [(x_2,y_2), (u_2,v_2)],\ldots, [(x_k,y_k), (u_k,v_k)]$
IF for all i, $y_i=u_i$ THEN Return "pseudo" ELSE Return "random".

Pr(T outputs "pseudo" | sequence is pseudo-random) = 1
Pr(T outputs "pseudo" | sequence is random) = $1/2^{kn}$

(c) Show that $\{ \pi_{k1,k2} : \{0,1\}^{2n} \rightarrow \{0,1\}^{2n} \}_{k1,k2}$ is not a PRΠG.

ANSWER:
Indeed we show that it is not a PRΦG. First notice that
$\pi_{k1,k2}(x,y) = \pi_{k1}(\pi_{k2}(x,y)) = \pi_{k1}(y , x \oplus f_{k2}(y)) = [x \oplus f_{k2}(y) , y \oplus f_{k1}(x \oplus f_{k2}(y))]$
and thus for fixed y, $\pi_{k1,k2}(x_i,y) = [x_i \oplus f_{k2}(y) , y \oplus f_{k1}(x_i \oplus f_{k2}(y))]$ the first component of the output is always a modified version of x_i, modified by a fixed constant.
Consider the following distinguisher T:

On input $[(x_1,y), (u_1,v_1)], [(x_2,y), (u_2,v_2)],\ldots, [(x_k,y), (u_k,v_k)]$
IF for all i>1, $u_i \oplus u_1 = x_i \oplus x_1$ THEN Return "pseudo" ELSE Return "random".

Pr(T outputs "pseudo" | sequence is pseudo-random) = 1
Pr(T outputs "pseudo" | sequence is random) = $1/2^{(k-1)n}$

(d) Explain the relationship between these permutations and DES.

ANSWER:
DES contains 16 recursions of $\pi_{ki}(x,y)$ for keys k1,k2,…,k16 obtained by the key-scheduling algorithm, and a particular family of functions.

(e) Show how to compute their inverses $\pi^{-1}_k(x,y)$, $\pi^{-1}_{k1,k2}(x,y)$, $\pi^{-1}_{k1,k2,k3}(x,y)$.

ANSWER:
- $\pi^{-1}_k(u,v) = [\, v \oplus f_k(u) \,,\, u \,]$
- $\pi^{-1}_{k1,k2}(u,v) = \pi^{-1}_{k2}(\pi^{-1}_{k1}(u,v))$
- $\pi^{-1}_{k1,k2,k3}(u,v) = \pi^{-1}_{k3}(\pi^{-1}_{k2}(\pi^{-1}_{k1}(u,v)))$

proof:
$\pi^{-1}_k(\pi_k(x,y)) = \pi^{-1}_k(\, y \,,\, x \oplus f_k(y) \,) = [\, x \oplus f_k(y) \oplus f_k(y) \,,\, y \,] = [\, x, y \,]$

$\pi^{-1}_{k1,k2}(\pi_{k1,k2}(x,y)) = \pi^{-1}_{k2}(\pi^{-1}_{k1}(\pi_{k1}(\pi_{k2}(x,y)))) = \pi^{-1}_{k2}(\pi_{k2}(x,y)) = [\, x, y \,]$

$\pi^{-1}_{k1,k2,k3}(\pi_{k1,k2,k3}(x,y)) = \pi^{-1}_{k3}(\pi^{-1}_{k2}(\pi^{-1}_{k1}(\pi_{k1}(\pi_{k2}(\pi_{k3}(x,y)))))) = \pi^{-1}_{k3}(\pi_{k3}(x,y)) = [\, x, y \,]$

(f) Explain how Alice and Bob could share a secret key k1,k2,k3 and use both $\pi_{k1,k2,k3}$ and $\pi^{-1}_{k1,k2,k3}$ to do encryption/decryption of bit-strings of size 2n. What would be the security properties of such a system ? (Make the strongest possible statement).

ANSWER:
Let $P=C=\{0,1\}^{2n}$ be the plaintext and ciphertext spaces. Take $E_{k1,k2,k3} = \pi_{k1,k2,k3}$ as encryption function and $D_{k1,k2,k3} = \pi^{-1}_{k1,k2,k3}$ as decryption function. Clearly, this satisfies the definition of a cryptosystem since $\pi^{-1}_{k1,k2,k3}(\pi_{k1,k2,k3}(x,y)) = [\, x, y \,]$ for all x,y. This cryptosystem is secure against chosen plaintext attacks since by definition of the PRΠG even after seeing as many chosen plaintext-ciphertext pairs $[(x,y) \,,\, E_{k1,k2,k3}(x,y)\,]$ as wanted, it remains difficult to predict anything about any other plaintext-ciphertext pair.

(g) BONUS QUESTION
Explain how to make this system even more secure.
(HINT: think of probabilistic encryption)

ANSWER:
Let $P=\{0,1\}^n$ and $C=\{0,1\}^{2n}$ be the plaintext and ciphertext spaces.
Take $E_{k1,k2,k3}(x) = \pi_{k1,k2,k3}(x,y)$ for a random y in $\{0,1\}^n$ as encryption function and $D_{k1,k2,k3} = \pi^{-1}_{k1,k2,k3}|_x$ (the first component of) as decryption function. Clearly, this satisfies the definition of a cryptosystem since $D_{k1,k2,k3}(E_{k1,k2,k3}(x)) = x$ for all x. This cryptosystem is secure against chosen plaintext as above. Moreover it is semantically secure since given two encryptions no distinguisher can tell whether they result from the same message or not.