Cosi 171a Fall 2004 Quiz 3 Solutions

Old Stuff:

(1) State the definition of *perfect secrecy* in a cipher. $P(X|Y) = P(X)$.

(2) Assuming uniform keys independent of X, show perfect secrecy implies $P(Y|X) = P(Y)$
$P(Y|X) = P(X,Y)/P(X) = P(Y|X)P(X)/P(X) = P(Y)$.

(3) Suppose we choose a set of n keys uniformly and independently with replacement from a keyspace of size K. Write an expression for the exact probability that a particular key is absent from the set. Approximate the probability, using a power of e.
$(1-1/K)^n = (1-1/K)^{nK/K} \approx e^{-K/n}$.

(4) Using RSA, show how A encrypts message x to B with both privacy and signature. $y = (x, h(x)^{d_A} \bmod n_a)^{e_B} \bmod n_B$

(5) Use the Pollard Rho algorithm with initial value 1 and iteration function $f(x) = x^2 + 1 \mod 55$ to factor 55.
$(1,1),\ \gcd(0,55) = 0;\ (2,5),\ \gcd(3,55) = 1;$
$(5,17),\ \gcd(12,55) = 1,\ (26,6),\ \gcd(20,55) = 5.$

Euler's Criteria:

(1) What is Euler's criterion that x be a square mod p? $x^{(p-1)/2} \equiv 1 \bmod p$ (Theorem 5.9, p. 174)

(2) What is Euler's criterion that g be a generator mod p? $g^{(p-1)/2} \not\equiv 1 \bmod p$ for all prime q which divide $p-1$. (Theorem 5.8, p. 166)

Diffie-Hellman Key Exchange:

Suppose $p = 101$ and generator $\gamma = 2$. Alice chooses private key $a = 3$, Bob chooses private key $b = 3$. What becomes their shared secret key?
$(2^3)^3 = 2^9 = 512 \equiv 7 \bmod 101$.

Shamir Secret Sharing:

(1) $d+1$ shares are necessary to determine a polynomial of degree d.

(2) Reconstruct the polynomial whose shares are $(1,9),(2,7),(10,3) \bmod 11$. The value 10 was used because $10 \equiv -1 \bmod 11$; also $6^{-1} \equiv 2,\ 3^{-1} \equiv 4$.

$$\begin{aligned}
f(x) &\equiv 9\frac{(x-2)(x+1)}{(1-2)(1+1)} + 7\frac{(x-1)(x+1)}{(2-1)(2+1)} + 3\frac{(x-1)(x-2)}{(-1-1)(-1-2)} \\
&\equiv 9\frac{x^2-x-2}{-2} + 7\frac{x^2-1}{3} + 3\frac{x^2-3x+2}{6} \\
&\equiv \frac{9}{9}(x^2-x-2) + 7\cdot 4(x^2-1) + 3\cdot 2(x^2-3x+2) \\
&\equiv (x^2-x-2) + 6(x^2-1) + 6(x^2-3x+2) \\
&\equiv 2x^2 - 8x + 4 \equiv 2x^2 + 3x + 4 \bmod 11
\end{aligned}$$

El-Gamal Encryption:

(1) Define El Gamal encryption of $x \in \mathbb{Z}_p$, stating which values are public or private, fixed or random.
Private: fixed key a, secret random r
Public and Fixed: prime p, generator $g \bmod p$, $g^a \bmod p$.
$y = (g^r, x(g^a)^r) \bmod p$.

(2) Is El Gamal vulnerable to chosen plaintext attack? No: The random g^r changes with each encryption, so even if an adversary gets $y = (g^r, (g^a)^r)$, the encryption of $x = 1$, the knowledge of g^{ar} is useless when r changes.

Interactive Proofs: Fill in the blanks indicated by "#":
Claim $x \in QR(n)$**:**
For round $i \leftarrow 1$ to $\lg n$
P sends to V random r_i^2
V sends to P random challenge $b_i \in \{0, 1\}$
P returns to V $s_i \equiv \begin{cases} \sqrt{r_i^2} & \text{if} \quad b_i = 0 \\ \sqrt{xr_i^2} & \text{if} \quad b_i = 1. \end{cases}$
V checks that $s_i^2 = x^{b_i} r_i^2$.

Why can't P cheat? If $x \notin QR(n)$ P can't provide both square roots.

Claim graph $G_0 \not\approx G_1$**:**
For round $i \leftarrow 1$ to $|G|$
V sends to P random challenge $\Pi_i G_0$ or $\Pi_i G_1$
P returns to V $s_i \equiv \begin{cases} 0 & \text{if} \quad s_i = \Pi_i G_0 \\ 1 & \text{if} \quad s_i = \Pi_i G_1 \end{cases}$
V checks that P was right.
If the graphs *are* isomorphic, P can only guess which one V permuted.
What knowledge might V gain? She might learn a random graph isomorphic to G_0 or G_1, but she could have generated one herself.

Zero-Knowledge:
Change the following IP to deny V the factorization of chosen numbers.
Claim: P claims to be able to factor composites.
For round $i \leftarrow 1$ to $\lg n$
V computes and sends to P random $n_i = p_i q_i$
P returns to V a commitment to p_i; demands that V show p_i
V sends p_i to P, proving that she knew it.
P opens his commitment.
V verifies that the committed value divides n.
The last step is necessary because P might have committed to q_i.

Quantum Cryptography:

(1) Complete this BB84 interaction, using "?" for "indeterminate":

Alice sends	$\uparrow$	$\nearrow$	$\nearrow$	$\rightarrow$	$\nearrow$	$\rightarrow$	$\nearrow$	$\uparrow$
Bob tries these bases and tells them to Alice	$+$	$+$	$\times$	$\times$	$+$	$+$	$\times$	$\times$
Bob reads	1	?	0	?	?	0	0	?
Alice confirms	1	0	1	0	0	1	1	0
Shared One Time Pad	1		0			0	0	

(2) To detect eavesdropping or tampering, Bob tells Alice some of his one-time-pad bits; if any are incorrect they discard the OTP. If they "waste" k OTP bits, what is their probability of detecting eavesdropping/tampering?

Eve escapes detection when 1) she guesses the correct basis, or 2) She uses the wrong basis, but Bob gets the correct binary value by chance. So Eve evades detection with probability $1/2 + 1/4 = 3/4$ Her chance of evading detection k times is $(3/4)^k$. The chance of catching her is $1 - (3/4)^k$.