Math 3210H — Cryptography – Final Exam
Monday, April 20, 2009.

1. Alice and Bob want to use the *El Gamal* cryptosystem. They choose the prime $p = 19$ and the base $g = 2$.

($\frac{5}{100}$) (a) Alice chooses private key $a = 5$. What is her public key A?

Solution: $A = 2^5 = 32 \underset{19}{\equiv} \boxed{\text{-6}}$. □

($\frac{5}{100}$) (b) Bob encrypts the message $m = 2$ using the ephemeral key $k = 3$. What is the cyphertext?

Solution: $c_1 = g^k = 2^3 = 8$.

$A^k = (-6)^3 = -6 \cdot 36 \underset{19}{\equiv} (-6) \cdot (-2) = 12$.

$c_2 = A^k \cdot m = 12 \cdot 2 = 24 \underset{19}{\equiv} 5$. Thus, the cyphertext is $\boxed{(8, 5).}$ □

($\frac{5}{100}$) (c) Alice receives cyphertext $(c_1, c_2) = (3, 7)$. What is the plaintext? (*Hint.* $-5 \cdot 243 \underset{19}{\equiv} 1$).

Solution: $c_1^a = 3^5 = 243$. Thus, $(c_1^a)^{-1} = 243^{-1} \underset{19}{\equiv} -5$ (by the hint). Thus, $m = (c_1^a)^{-1} \cdot c_2 = -5 \cdot 7 = -35 \underset{19}{\equiv} \boxed{3}$. □

($\frac{15}{100}$) 2. Formulate a '(wo)man-in-the-middle' attack for the RSA public key cryptosystem.

(*Note:* Assume that Eve can intercept and tamper with *all* communications between Alice and Bob, including Alice's initial attempt to transmit her public key data.)

Solution: In the RSA cryptosystem, Alice chooses two secret primes p and q a secret decryption exponent d coprime to $(p-1)(q-1)$. She then computes the inverse e of d, mod $(p-1)(q-1)$, and broadcasts e and $N = pq$. The pair (N, e) is Alice's public key. To encrypt a message m, Bob computes $c = m^e$ and sends it to Alice. To decrypt the cyphertext c, Alice computes $m' = c^d = m^{ed} \underset{N}{\equiv} m$.

Suppose Eve can control the communications between Bob and Alice. First, she intercepts Alice's public key (N, e) and substitutes a fake public key (N', e'), which she sends on to Bob. Bob then encrypts m using the fake key, to produce cyphertext $c' = m^{e'}$. Eve intercepts c' and decrypts it (by computing $(c')^{d'} = m^{e'd'} = m$). Then she re-encrypts it using Alice's key (to obtain $c = m^e$), and sends this message onto Alice. Alice is able to decrypt this new cyphertext using her own private key —she is unaware that the message was intercepted and decrypted by Eve en route.

Remark. If Alice is able to broadcast her public key on a channel which Eve does not control (e.g. the radio), then the man-in-the-middle attack fails. This shows one of the advantages of public key cryptography: if you can get access to a public channel even once (even an insecure one) then you can thwart any later attempt at a man-in-the-middle attack. □

($\frac{10}{100}$) 3. Show that $5x^3 + 10x^2 + \ln(x) = \mathcal{O}(x^3)$.

Solution: We have

$$\begin{aligned}\lim_{x\to\infty} \frac{5x^3 + 10x^2 + \ln(x)}{x^3} &= \lim_{x\to\infty} 5 + \frac{10}{x} + \frac{\ln(x)}{x^3} = 5 + 0 + \lim_{x\to\infty} \frac{\ln(x)}{x^3} \\ &\underset{(\mathrm{H})}{=} 5 + \lim_{x\to\infty} \frac{1/x}{3x^2} = 5 + 0 = 5 < \infty,\end{aligned}$$

where (H) is by l'Hospital's rule. □

($\frac{10}{100}$) 4. Factor 391 into primes, use Pollard's $(p-1)$ factoring algorithm and the following information:

$$\begin{aligned} 2^{2!} - 1 &= 3 &&\underset{391}{\equiv} 3; \\ 2^{3!} - 1 &= 63 &&\underset{391}{\equiv} 63; \\ 2^{4!} - 1 &= 16777215 &&\underset{391}{\equiv} 187; \\ 2^{5!} - 1 &= [huge] &&\underset{391}{\equiv} 34; \\ 2^{6!} - 1 &= [huge] &&\underset{391}{\equiv} 238; \end{aligned}$$

Solution: By simple computation, $\gcd(2^{4!} - 1, 391) = 17$. Thus, 17 is a divisor of 391. Indeed, $391/17 = 23$. Since both 17 and 23 are prime, we're done: $\boxed{391 = 17 \cdot 23}$. □

($\frac{15}{100}$) 5. Let p be a prime number and let $g \in \mathbb{Z}^*_{/p}$ be a primitive root, mod p. Let $a \in \mathbb{Z}^*_{/p}$ and let $L := \log_g(a)$ be its discrete logarithm. Prove that

$$(-1)^L = \left(\frac{a}{p}\right).$$

Solution: In the proof of Proposition 3.60, we showed that g^L is a quadratic residue if and only if L is even. Thus, we have

$$\Big((-1)^L = 1\Big) \iff \Big(L \text{ is even}\Big) \iff \Big(g^L \text{ is a quadratic residue}\Big) \iff \left(\left(\frac{a}{p}\right) = 1\right).$$

Likewise, $\Big((-1)^L = 1\Big) \iff \left(\left(\frac{a}{p}\right) = -1\right)$. □

6. Recall that a function $h : [0,1] \longrightarrow \mathbb{R}$ is *concave* if, for any distinct $x_1, x_2 \in [0,1]$, and any $r_1, r_2 \in (0,1)$ with $r_1 + r_2 = 1$, we have $h(r_1x_1 + r_2x_2) > r_1h(x_1) + r_2h(x_2)$. If h is differentiable, then h is concave if and only if $h'' < 0$ (you don't need to prove this).

Define $h : [0,1] \longrightarrow \mathbb{R}$ by $h(x) = -x \cdot \log_2(x)$.

($\frac{5}{100}$) (a) Compute $h''(x)$. Show that $h''(x) < 0$ for all $x \in [0,1]$.

Solution: Let $\lambda := \ln(2)$. Then $\log_2(x) = \ln(x)/\lambda$. Thus $h'(x) = -\log_2(x) - \frac{x}{\lambda x} = -\log_2(x) - 1/\lambda$. Thus, $h''(x) = -\log_2'(x) = \boxed{-1/\lambda x}$. Clearly, $-1/\lambda x < 0$ for all $x \in [0,1]$. □

(b) Let $\Delta^N := \left\{ \mathbf{p} \in \mathbb{R}_+^N \; ; \; \sum_{n=1}^N p_n = 1 \right\}$ be the set of N-dimensional *probability vectors*.
($\frac{10}{100}$) Recall that we define the entropy function $H : \Delta^N \longrightarrow \mathbb{R}_+$ by

$$H(\mathbf{p}) \quad := \quad -\sum_{n=1}^N p_n \cdot \log_2(p_n).$$

Show that H is *concave* on Δ^N. That is, for any distinct $\mathbf{p}^1, \mathbf{p}^2 \in \Delta^N$, and any $r_1, r_2 \in (0,1)$ with $r_1 + r_2 = 1$, we have

$$H(r_1\mathbf{p}^1 + r_2\mathbf{p}^2) \quad > \quad r_1 H(\mathbf{p}_1) + r_2 H(\mathbf{p}_2).$$

(Intuitively, this means that a 'mixture' of two random variables has more entropy than the average entropy of the two random variables considered separately).

Solution: Let $h : [0,1] \longrightarrow \mathbb{R}$ be as in part (a). Then $H(\mathbf{p}) = \sum_{n=1}^N h(p_n)$. Thus,

$$\begin{aligned} H(r_1\mathbf{p}^1 + r_2\mathbf{p}^2) &= \sum_{n=1}^N h(r_1 p_n^1 + r_2 p_n^2) \underset{(*)}{>} \sum_{n=1}^N r_1 h(p_n^1) + r_2 h(p_n^2) \\ &= r_1 \sum_{n=1}^N h(p_n^1) \; + \; r_2 \sum_{n=1}^N h(p_n^2) \quad = \quad r_1 H(\mathbf{p}_1) + r_2 H(\mathbf{p}_2), \end{aligned}$$

as desired. Here $(*)$ is because h is concave, because $h'' < 0$. □

7. Let Ω be a probability space. Let $\mathcal{X}$ and $\mathcal{Y}$ be finite sets. Let $X : \Omega \longrightarrow \mathcal{X}$ and $Y : \Omega \longrightarrow \mathcal{Y}$
($\frac{20}{100}$) be random variables Suppose $\mathcal{H}(X|Y) = \mathcal{H}(X)$. Does this necessarily mean that X is independent of Y? If your answer is 'yes', then give a proof. If your answer is 'no', then give a counterexample.

Solution: The answer is 'yes'. We will prove this by contrapositive. Suppose X is *not* independent of Y; then we will show that $H(X|Y) < H(Y)$ (Intuitively: if X is not independent of Y, then knowing the value of Y reveals some information about X).

For all $y \in \mathcal{Y}$ and $x \in \mathcal{X}$, let $f_{X|y}(x)$ be the conditional probability that $X = x$, given that $Y = y$. Let $f_X(x)$ be the unconditional probability that $X = x$. Then

$$f_X(x) \quad = \quad \sum_{y \in \mathcal{Y}} f_Y(y) \cdot f_{X|y}(x).$$

In other words, the probability distribution f_X is a convex combination of the conditional probability distributions $f_{X|y}$:

$$f_X \quad = \quad \sum_{y \in \mathcal{Y}} f_Y(y) \cdot f_{X|y} \tag{1}$$

Now, if X is *not* independent of y, then there exists some $y \in \mathcal{Y}$ such that $f_X \neq f_{X|y}$. Thus means that there exists $y_1, y_2 \in \mathcal{Y}$ such that $f_{X|y_1} \neq f_{X|y_2}$. The function H is concave, by problem #5(b). Thus, Jensen's Inequality applied to eqn.(1) implies that

$$H(X) \quad := \quad H(f_X) \quad > \quad \sum_{y \in \mathcal{Y}} f_Y(y) \cdot H(f_{X|y}). \tag{2}$$

But by definition,

$$\mathcal{H}(X|Y) \quad := \quad -\sum_{y \in \mathcal{Y}} f_Y(y) \cdot \sum_{x \in \mathcal{X}} f_{X|y}(x) \cdot \log_2 \left[f_{X|y}(x) \right] \quad = \quad \sum_{y \in \mathcal{Y}} f_Y(y) \cdot H(f_{X|y}). \tag{3}$$

Combining equations (2) and (3), we conclude that $H(X) > \mathcal{H}(X|Y)$. □