NT-Cryptography MAT4930 *7554* **Quizzes Q** 29Sep2010

Q1: Wedn. 26 Jan $N := \varphi(100) =$ ______. So $\varphi(N) =$ ______.
EFT says that $3^{165} \equiv_N$ ______ $\in [0..N)$. Hence (by EFT) last two digits of $7^{[3^{165}]}$ are ______.

Q2: Fri. 28 Jan With $M := 22$ and $J := [0..M)$, use *repeated-squaring* to compute $6^{4096} \equiv_M$ ______ $\in J$. Since 4101 equals $2^{12} + 2^2 + 2^0$, the power $6^{4101} \equiv_M$ ______ $\in J$.
[*Hint:* Compute with symm. residues, and use periodicity.]

Q3: Mon. 31 Jan Define $G{:}[1..12]\circlearrowleft$ where $G(n)$ is the number of letters in the n^{th} Gregorian month. So $G(2) = 8$, since the 2^{nd} month is "February". The only fixed-point of G is ______. The *set* of posints k where $G^{\circ k}(12) = G^{\circ k}(7)$ is ______.
[January, February, March, April, May, June, July, August, September, October, November, December]

Q4: Wedn. 2 Feb With $A := 29$, $B := 20$, $U := A{\cdot}B = 580$, let $\mathbf{J}$ be $(-290..290]$. There is a ring-iso $F{:}\mathbb{Z}_A \times \mathbb{Z}_B \to \mathbb{Z}_U$ sending (α, β) to $\langle G\alpha + H\beta \rangle_U$, using magic numbers $G=$ ______ $\in \mathbf{J}$ and $H=$ ______ $\in \mathbf{J}$. A mod-U root of poly $h(x) := 20{\cdot}[x+10]^3 + 29{\cdot}[x-2]$ is (______, ______) $\overset{F}{\mapsto}$ ______ $\in \mathbf{J}$.

Q5: Wedn. 9 Feb **i** Let $L() := \log_2()$. The ***distribution entropy*** of probability-vector $\left(\frac{1}{8}, \frac{1}{32}, \frac{1}{32}, \frac{1}{32}, \frac{25}{32}\right)$ equals ______.

ii With $A := 29$, $B := 20$, $U := A{\cdot}B = 580$, let $\mathbf{J}$ be $(-290..290]$. There is a ring-iso $F{:}\mathbb{Z}_A \times \mathbb{Z}_B \to \mathbb{Z}_U$ sending (α, β) to $\langle G\alpha + H\beta \rangle_U$, using magic numbers $G=$ ______ $\in \mathbf{J}$ and $H=$ ______ $\in \mathbf{J}$. A mod-U root of poly $h(x) := 20{\cdot}[x+10]^3 + 29{\cdot}[x-2]$ is (______, ______) $\overset{F}{\mapsto}$ ______ $\in \mathbf{J}$.

Q6: Wedn. 23 Feb Bits $\langle 2\rangle 0 \langle 3\rangle 1 \langle 4\rangle 0 \langle 3\rangle 0 \langle 6\rangle 1 \langle 0\rangle \langle 7\rangle$ *decode* in Idx-form, e.g $\langle 7\rangle 1 \langle 3\rangle 1 \langle 9\rangle 0 \ldots \langle 3\rangle 1 \langle 0\rangle \langle 4\rangle$, to ______.
As 20 bits, it is ______ having used *Ziv* seeded with $\langle 0\rangle =$'', $\langle 1\rangle =$'1', and $\langle 2\rangle =$'0'.
Employing our fivebit-code, the 20 bits decode to symbols ______ ______ ______ ______.

Q7: Mon. 28 Feb Define the ***numeral map*** $h{:}[1..12]\circlearrowleft$, where $h(n)$ is the number of letters in the n^{th} numeral. So $h(12)$ equals 6, since "twelve" has 6 letters.
Compute the convolution $[h \circledast \boldsymbol{\mu}](10) =$ ______.

Let $g := \boldsymbol{\sigma}^{\circledast -1}$ [i.e, the convol-inverse of the divisor-sum fnc]. So $g(2) =$ ______, $g(9) =$ ______ and $g(18) =$ ______.

Q8: Fri. 4 Mar Using 32-symbol alphabet "`abc...z '.?!,`" mapped to $[0..32)$, the 27-character phrase

"`bpqzinpr?zmpqlupe?x nkwnczg`"

comes from cleartext which *undoubtedly* starts with "`a fine quiz`". The encryption affine-map is thus $\alpha \mapsto \big[[$ ______ $\cdot\, \alpha] +$ ______ $\big]$ mod-32. Decryption is $\beta \mapsto \big[[$ ______ $\cdot\, \beta] +$ ______ $\big]$ mod-32. The full cleartext is
______
______

Q9: Mon. 21 Mar Applying the Floyd cycle-finding (Tortoise & Hare) to a finite orbit which has tail $T := 3$ and eventual-period $L := 4$, yields *hitting time* $H=$ ______.

Q10: Fri. 4 Mar Solve *Some Of* the World's Problems.

§A Potential quiz problems

Some of these may appear on quizzes/exams; naturally, with different data. *Write **DNE** in a blank if the described object does not exist or if the indicated operation cannot be performed.*

PF Use Pollard-ρ to find a non-trivial factor of $N := 250997$, using seed $s_0 := 33287$ and map $f(x) := 1+x^2$. Make a nice table, labeled

Time | Tortoise | Hare | $s_{2k} - s_k$ | Gcd(??)

—*but **replace** the "??" with the correct expression.* You found non-trivial factor $E :=$ ________.

[*Fact:* Your table has ⩽4 lines.]

rs1 Sequence $\vec{\mathbf{s}} := (s_n)_{n=-\infty}^{\infty}$ is defined by recurrence

$$s_{n+2} = s_{n+1} + 3s_n, \quad \text{with initial-conditions } s_1 := -1 \text{ and } s_0 := 7.$$

With $\mathbf{v}_n := \begin{bmatrix} s_{n+1} \\ s_n \end{bmatrix}$, matrix $\mathsf{M} :=$ ________ satisfies $\forall k$: $\mathbf{v}_k = \mathsf{M}^k \mathbf{v}_0$. Henceforth in ring $\mathbb{Z}_{10} = [0..10)$, power $\mathsf{M}^{32} \equiv$ ________ and $s_{40} \equiv$ ________.

cr0 With $A := 29$, $B := 20$, $U := A \cdot B = 580$, let $\mathbf{J}$ be $(-290..290]$. There is a ring-iso $F: \mathbb{Z}_A \times \mathbb{Z}_B \to \mathbb{Z}_U$ sending (α, β) to $\langle G\alpha + H\beta \rangle_U$, using magic numbers $G=$ ________ $\in \mathbf{J}$ and $H=$ ________ $\in \mathbf{J}$. A mod-U root of poly $h(x) := 20 \cdot [x+10]^3 + 29 \cdot [x-2]$ is (________ , ________) $\overset{F}{\mapsto}$ ________ $\in \mathbf{J}$.

cr1 So $z=$ ________ is the smallest natnum satisfying

$$z \equiv_7 -2, \quad z \equiv_8 -1, \quad z \equiv_{11} 5, \quad z \equiv_{15} 12.$$

cr2 *Magic integers* $G_1=$ ________, $G_2=$ ________, $G_3=$ ________, each in $(-165..165]$, are st. mapping $g: \mathbb{Z}_6 \times \mathbb{Z}_5 \times \mathbb{Z}_{11} \to \mathbb{Z}_{330}$ is a ring-isomorphism, where

$$g((z_1, z_2, z_3)) := \left\langle z_1 G_1 + z_2 G_2 + z_3 G_3 \right\rangle_{330}.$$

Verify for <u>your</u> map: $g((1,1,1)) = 1$ and $[5 \cdot 11] \bullet\!| \; G_1$ and analogously for G_2 and G_3.

cr3 *Essay ques: Magic integers* $G_1=$ ____, $G_2=$ ____, $G_3=$ ________, $G_4=$ ________, each in $[0..1260)$, are st. $g: \mathbb{Z}_7 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \to \mathbb{Z}_{1260}$ is a ring-iso, where

$$g((z_1, z_2, z_3, z_4)) := \left\langle z_1 G_1 + z_2 G_2 + z_3 G_3 + z_4 G_4 \right\rangle_{1260}.$$

Now consider poly $h(x) := [x+59][x-1][x+83]$. Find all solutions to congruences $h(x) \equiv_M 0$, for $M = 7, 4, 9, 5$, displaying the *results* in a nice table. (Do **not** show work for this step.)

Now use your ring-iso to compute *all* solns x to $\boxed{h(x) \equiv_{1260} 0}$, displaying the results in a table which shows *which* 4tup each came from. There are (<u>not</u> counting multiplicities) $K:=$ ________ many solns. Explain your method well; then show **<u>one</u>** computation giving a root *different* (mod 1260) from $-59, 1, -83$.

sf According to class defn, circle those integers which are ***square-free***: $-8, -4, -2, 0, 1, 12, 27, 65$.

ℓ Poly $h(x) := \sum_{n=0}^{2} V_n x^n$ satisfies $h(1)=4$, $h(2)=9$, $h(-1)=6$. Then $V_0=$ ______, $V_1=$ ______, $V_2=$ ______.

m_5 $\mathsf{M} := \begin{bmatrix} 70 & 7 \\ 1 & 2 \end{bmatrix}$. Compute M^{-1} over these three fields. [Write your $\mathbb{Z}_p$ answers using symmetric residues.]

Over $\mathbb{Z}_5$: $\mathsf{M}^{-1}=$ ________. Over $\mathbb{Z}_7$: $\mathsf{M}^{-1}=$ ________.

Over $\mathbb{Q}$: $\mathsf{M}^{-1}=$ ________________.

mf1 Since $4800 = 2^6 \cdot 3^1 \cdot 5^2$, it has ________ many positive divisors. [Write ANS naturally as a product of integers.]

mf2 The divisor-sum $\boldsymbol{\sigma}(1500) =$ ________. Express your answer a product $p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots$ of primes to posint powers, with $p_1 < p_2 < \ldots$.

Definitions, and their application

Use $\mathbb{F}$ for a general field, and $\mathbf{V}$ is an $\mathbb{F}$-VS.

p_1 The ***distropy*** (distribution entropy) of a probability vector $\vec{\mathbf{v}} = (p_1, p_2, \ldots, p_N)$ is $\mathcal{H}(\vec{\mathbf{v}}) =$ ________.

p1 A polynomial $h(x)$ is ***monic*** IFF ....

[Imagine 3 blank lines].
....

p2 A polynomial $g(x,y,z)$ is ***homogeneous*** IFF

[Imagine 5 blank lines].
....

Coding

cH1 Suppose the letters A F H M N U have frequencies $\frac{12}{170}, \frac{46}{170}, \frac{38}{170}, \frac{18}{170}, \frac{15}{170}, \frac{41}{170}$, respectively. Construct the unique Huffman prefix-code with these frequencies; at each coalescing, use 0 for the less-probable branch and 1 for the more-probable. **Draw** the Huffman tree (large!). Label the branches and leaves with bits and letters. The name HUFFMAN encodes to

....

Examining the tree, what kind of *Being* is HUFFMAN?

Answering the question *"What're y'all?"*, message 10100010101001110100110111010*!* decodes to .... *!*

cH2 The Huffman code with letter-probabilities

$\mathcal{I}{:}\frac{12}{66}$ $\mathcal{M}{:}\frac{5}{66}$ $\mathcal{O}{:}\frac{7}{66}$ $\mathcal{R}{:}\frac{4}{66}$ $\mathcal{S}{:}\frac{32}{66}$ $\mathcal{T}{:}\frac{6}{66}$

codes these to bitstrings: $\mathcal{I}$: .... $\mathcal{M}$: ....

$\mathcal{O}$: .... $\mathcal{R}$: .... $\mathcal{S}$: .... $\mathcal{T}$: ....

Bitstring 11011011100110011110 decodes to ...., answering: "*What is Big Moose's name?*"

Essay1: Compute a Huffman code for these five symbols.

A: 4/27 ....

B: 1/27 ....

C: 14/27 ....

D: 2/27 ....

E: 6/27 ....

When coalescing, use "0" to go to the smaller-prob. word.

And MECL$(\frac{4}{27}, \frac{1}{27}, \frac{14}{27}, \frac{2}{27}, \frac{6}{27})$= .... bits.

ii Give the example (with picture) from class of a minimum expected-length code which is **not** a Huffman code. Argue that your code is indeed of MECL, and is not Huffman.

iii State the Huffman Coding thm from class. Sketch a proof of it; just show the main ideas. (And pictures)

As of 03Feb2011, we have not yet covered some of the following coding material.

cE1 Bitstring "0001000101111111101101001", via the Elias code, decodes to ...., a sequence of *natnums* [hint: gun-blip-blip], followed by noise-bits ....

Conv, Elias(84)= .... (bitstring)

cZ1 Using dictionary 0: ε, 1: "1", 2: "0", compute EnZiv(11001010)= ...., in ⟨**7**⟩1⟨**34**⟩0... notation. In bits, EnZiv(11001010) is

....

cZ2 Bits 0100101010010000111000110110110011 1 *decode* in Idx-form, e.g ⟨**7**⟩1 ⟨**3**⟩1 ⟨**9**⟩0 ... ⟨**3**⟩1 ⟨**0**⟩⟨**4**⟩, to

....

As 15 bits, it is ....

having used *Ziv* seeded with ⟨**0**⟩='', ⟨**1**⟩='1', and ⟨**2**⟩='0'.

Employing our fivebit-code, the 15 bits decode to symbols ....

Playing with fields

C1 Blanks∈ℝ. So $\frac{1}{2+3\boldsymbol{i}}$ = ... $+\boldsymbol{i}\cdot$[..........].

Thus $\dfrac{7-2\boldsymbol{i}}{2+3\boldsymbol{i}}$ = ... $+\boldsymbol{i}\cdot$[..........].

By the way, $|5-3\boldsymbol{i}|$ = ...

C2 Note $[1+\boldsymbol{i}]^{86} = [\quad\quad] + \boldsymbol{i}\cdot[\quad\quad]$.

[*Hint: Multiplying complexes multiplies their moduli, and adds their angles.*]

Geometric series

GS1 Compute the sum of this geometric series: $\sum_{\beta=3}^{\infty} [\text{-}1]^{\beta}\cdot[3/5]^{\beta} =$ ______.

GS2 For natural number K, the sum $\sum_{n=3}^{3+K} 4^n$ equals ______.

GS3 $\sum_{n=0}^{2} r^n = \frac{19}{25}$. So $r=$ ______ or **DNE**.

GS4 $\sum_{k=1}^{\infty} r^k = \frac{5}{8}$. So $r=$ ______ or **DNE**.

[*Hint:* The sum starts with k at **one**, not zero.]

GS5 Compute the sum of this geometric series: $\sum_{n=0}^{\infty} \left[\frac{4}{2+3\boldsymbol{i}}\right]^n =$ ______.

GS6 Compute the sum of this geometric series: $\sum_{k=0}^{\infty} \left[\frac{2+3\boldsymbol{i}}{4}\right]^k =$ ______.