COMP-649A 2009 Homework set #1

Due Tuesday February, 3 2009 in class

A. ISBN code and Luhn algorithm

The **ISBN** numbers (codewords) that we find on all books originate from a code over $\mathbf{F_{11}}$ with alphabet **{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, X }** where "**X**" stands for 10. This code is linear and its parameters are $\mathbf{[10,k,d]_{11}}$.

[10%] **1)** Use a bunch of books and determine the generating matrix of this code (provide the book titles and **ISBN** numbers that you used). Determine the values of **k** and **d** for this code.

[5%] **2)** For extra credit, find the smallest number of books that have linearly dependant ISBN numbers (provide the book titles and ISBN numbers that you used).

[10%] **3)** Show that the **ISBN** code has the extra property that for any **ISBN** codeword $\mathbf{a=(a_1,a_2,\ldots,a_{10})}$ if $\mathbf{a_i}$ and $\mathbf{a_j}$ are distinct symbols then the word $\mathbf{w=(w_1,w_2,\ldots,w_{10})}$ is never a codeword, where $\mathbf{w_k=a_k}$ for **k=1,2,3,…,10** except for **k=i,j** where instead $\mathbf{w_i=a_j}$ and $\mathbf{w_j=a_i}$.

[15%] **4)** The digits of a credit card number satisfy a similar property. However the computations for a credit card are performed mod 10 (not 11). Using some credit card numbers find the parity check matrix of credit cards (known as Luhn's algorithm) and show that every transposition (XY to YX) is detectable expect for one pair. What is that pair ? Is this really a linear code ??

PS in order to get a true satisfaction from figuring this out by yourself, I strongly suggest you do got use *Google* to find these answers…

B. BB84 channels

Let Alice and Bob share a random variable **W** uniformly distributed over all n-bit strings. Assume Eve, the eavesdropper is allowed to choose to see each bit of **W** through one of the following channels, parameterized by angle **@**

$$\mathbf{V_i} = \begin{cases} \mathbf{BSC_{\sin^2(@)}(W_i)} & \text{with probability } ½ \\ \mathbf{BSC_{\sin^2(\pi/4-@)}(W_i)} & \text{with probability } ½. \end{cases}$$

Moreover, Eve knows for each bit which of the two possibilities actually occurred. We have seen in class the extreme cases where **@=0** and where **@=π/8**.

[15%] Show that the value of **@**, $\mathbf{0 \le @ \le \pi/8}$, which is most resistant to privacy amplification is **@=0**.

C. Secret Sharing

Consider the notion of secret sharing among a set of **n** users $\mathbf{U_1,\ldots,U_n}$. Let **S** be a secret chosen from a set of **Q** elements. A set of **n** shares $\mathbf{S_1,\ldots,S_n}$ will be distributed among the users, each $\mathbf{U_i}$ obtaining only $\mathbf{S_i}$. The **n** people choose some parameter $\mathbf{k \le n}$ such that any subset of fewer than **k** people have no clue about **S** from their shares, while any set of **k** or more people can determine exactly what **S is**. We call such a scheme an **[n,k]** threshold secret sharing scheme.

[10%] **1)** Give a formal definition using information theory that specifies the threshold property mentioned above.

[20%] **2)** If **Q** is a prime power explain the relation between **[n,k]** threshold secret sharing schemes and Reed-Solomon Codes over the field $\mathbf{F_Q}$. If **Q** is not a prime power, how can we still use Reed-

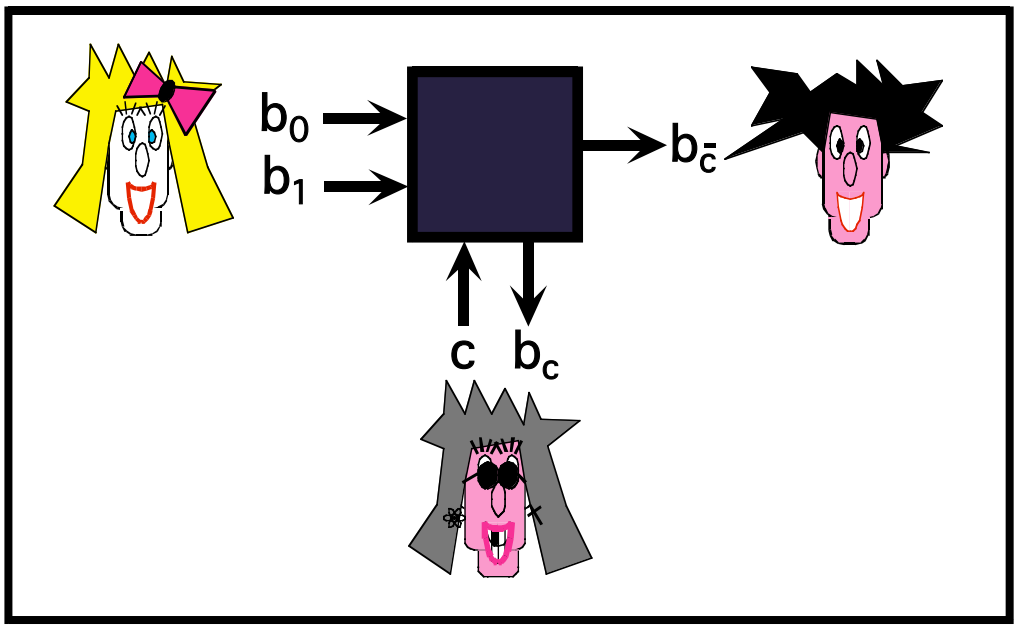
…more on back

Solomon codes to obtain **[n,k]** threshold secret sharing schemes? If some users are dishonest about their own share, how can we still recover the secret **S** ??

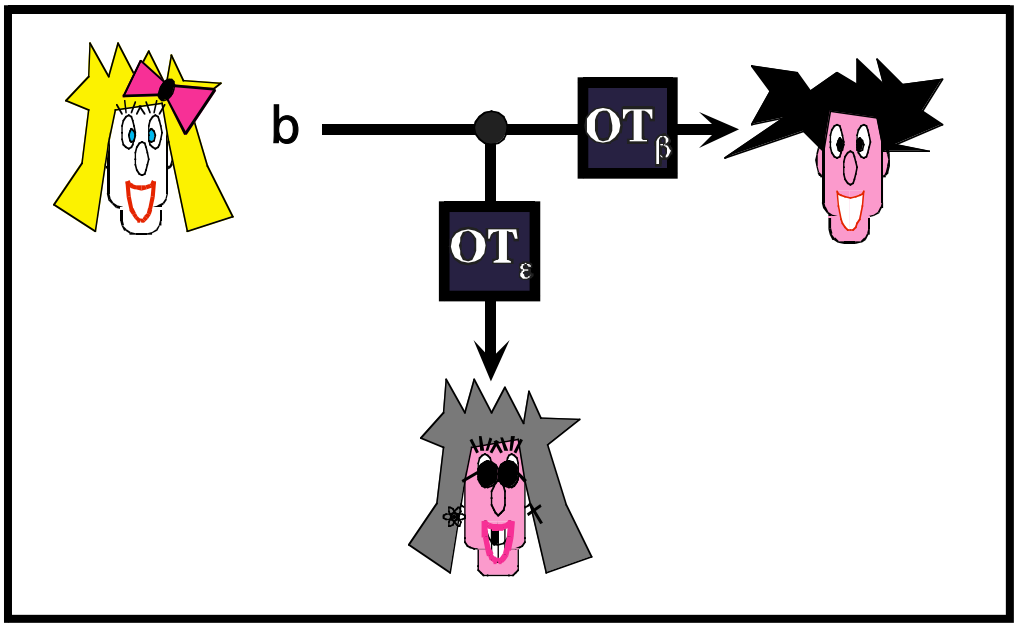
D. Chunnels

For each of the following situations, show how the honest Alice and Bob (who have access to an authenticated public channel) can take advantage of the insecure communication channel to exchange a secret key unknown to the eavesdropper Eve:

[10%] **1)**



[10%] **2)** Here, the probabilities β and ε of transmitting a bit are arbitrary (but fixed and known to everybody) and the OTs are independent.



…more on back