University of Wisconsin-Madison
Department of Electrical and Computer Engineering
CS/ECE/Math 435 - Introduction to Cryptography, Spring Semester 2021
Midterm Exam Formula Sheet

(i) Euler's Phi Function (excerpted from Bach notes p. 8-1):

$$\varphi(N) = N\left(1 - \sum_{p|N} 1/p + \sum_{p,q|N} 1/pq - \cdots\right) = N\prod_{p|N}(1 - 1/p).$$

(ii) Jordan's formula for the number of invertible matrices on $\mathbf{Z}_N$ (excerpted from Bach notes p. 8-2):

Around 1870, Jordan proved that there are

$$N^{n^2}\prod_{p|N}(1 - 1/p)(1 - 1/p^2)\cdots(1 - 1/p^n)$$

invertible $n \times n$ matrices over $\mathbf{Z}_N$.

(iii) expansion of determinant via co-factors:
BACKGROUND: Let A be a square nxn matrix. First observe that for the scalar case (1x1 matrix), A=a, det(a)=a. Then the (i,j) ***minor,*** denoted A_{ij}, is the (n−1)×(n−1) matrix obtained from A by deleting the ith row and the jth column. The (i, j) ***cofactor*** C_{ij} is defined in terms of the minor by

$$C_{ij}=(-1)^{i+j}\det(A_{ij}).$$

COFACTOR EXPASION FORMULA FOR DETERMINANT (by row):
Let A be an n×n matrix with entries a_{ij}.

1. *For any row index number i=1,2,...,n, we have*

$$\det(A) = \sum_{j=1}^{n} a_{ij}C_{ij} = a_{i1}C_{i1} + a_{i2}C_{i2} + \cdots + a_{in}C_{in}$$

*This is the **cofactor expansion along the ith row.***

(iv) Cramer's rule for matrix inverse:
Let A be a square nxn matrix. The inverse of A, A^{-1}, is given by
$A^{-1} = (\det(A))^{-1}$ x AdjugateMatrix(A)

where AdjugateMatrix(A) has j^{th}, i^{th} element equal to the i^{th},j^{th} cofactor of A (see definition of cofactors above, and note the carefully the role of indices i and j).

(v) the Gaussian integral with associated one standard deviation and two standard deviation probability values (excerpted from Bach notes pp. 10-2, 10-3):

$$\Pr[\frac{C-\mu}{\sigma} < a] \to \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{a} e^{-t^2/2} dt$$

Values of the integral (called the Gaussian or normal integral) are tabulated in books on probability and statistics.

Consequently, we expect to see

$$np - \sqrt{np(1-p)} \leq \text{ count of } x\text{'s } \leq np + \sqrt{np(1-p)}$$

about 68% of the time, and

$$np - 2\sqrt{np(1-p)} \leq \text{ count of } x\text{'s } \leq np + 2\sqrt{np(1-p)}$$

about 96% of the time.

(vi) Index of Coincidence (excerpted from Bach notes p. 12-1):

Let there be f_i occurrences of symbol i.

$$\mathrm{IC} = \frac{\sum_i f_i(f_i-1)/2}{n(n-1)/2} = \frac{\sum_i f_i(f_i-1)}{n(n-1)}$$

(vii) Expectation-based estimator for cipher period (excerpted from Bach notes p. 12-3; recall lecture used different notation of m_E for this quantity):

$$\hat{m} = \frac{n(\kappa_S - \kappa_R)}{(n-1)\hat{\mathrm{IC}} - n\kappa_R + \kappa_S}$$

(viii) definition of entropy, H (excerpted from Bach notes p. 14-1):

$$H(\{p_i\}) = -\sum_i p_i \log p_i.$$

(ix) key equivocation E_n (excerpted Bach notes p. 15-1):

$$E_n = H(P_n) + H(K) - H(C_n)$$

(x) $\log_2(x)$ expressed in terms of natural ln(x): $\log_2(x) = 1.4427\ln(x)$
{ observe that $1.4427 = \log_2(e)$ }