

Cryptography CS 555

Lecture 6 Part B



Enigma Machine, Birthday Paradox & Repeating
Ciphertext Blocks

Lecture Outline

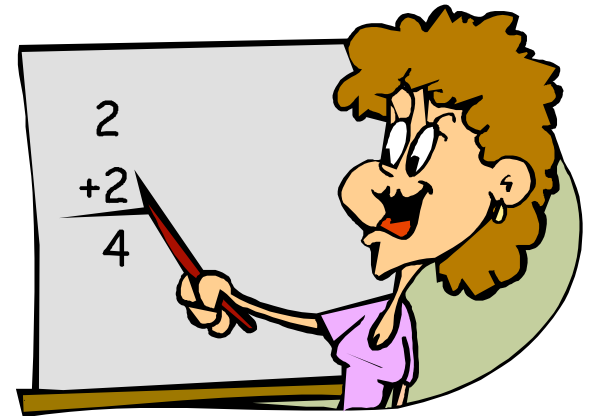
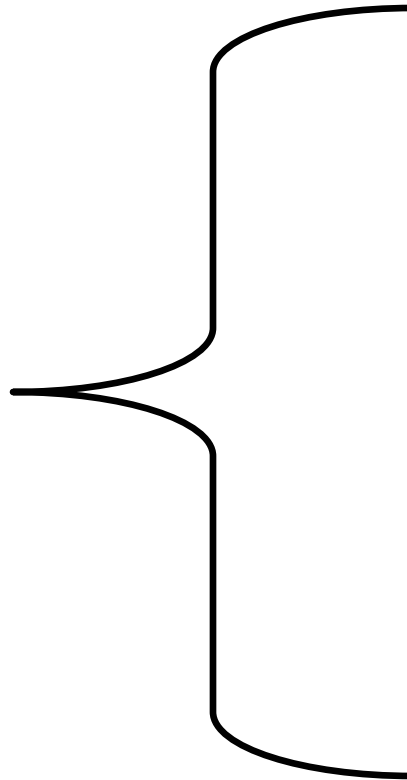
- Enigma machine
- Birthday Paradox
- Repeating ciphertext blocks in block cipher encrypting modes



On Attacking Enigma Machine

- The previous description of Enigma machine in class was incomplete, it does not include the reflector feature.
- The reflector makes the cipher invert itself
 - decryption the same as encryption, i.e., encryption twice gives one the plaintext
- Without the reflector, the chains won't be affected by the plugboard at all
- With the reflector, the shape of the chains won't be affected.

Begin Math



Birthday Paradox

- Given a group of people, what is the minimum number of people such that two will share the same birthday with probability > 0.5 .



General Problem

- Given a random variable that is an integer with uniform distribution between 1 and n and a selection of k instances, $k < n$ of the random variable, what is the probability $P(n, k)$ that there is at least one duplicate?

Calculating $P(365,k)$

- Pick k random days out of 365, what is the probability of no collision
- The number of ways of no collision
 - $365 \times 364 \times \dots \times (365 - k + 1) = 365! / (365-k)!$
- The total number of ways for picking
 - 365^k
- $P(365,k) = 1 - 365! / ((365-k)! 365^k)$
- $P(365,23) = 0.5073$

Solution to the general problem

$$\begin{aligned} P(n, k) &= 1 - \frac{n!}{(n-k)! n^k} \\ &= 1 - \left[\frac{n(n-1)\cdots(n-k+1)}{n^k} \right] \\ &= 1 - \left[\frac{n}{n} \bullet \frac{n-1}{n} \bullet \frac{n-2}{n} \bullet \dots \bullet \frac{n-(k-1)}{n} \right] \\ &= 1 - \left[\left(1 - \frac{1}{n}\right) \bullet \left(1 - \frac{2}{n}\right) \bullet \dots \bullet \left(1 - \frac{k-1}{n}\right) \right] \\ &\geq 1 - \left[e^{-\frac{1}{n}} \bullet e^{-\frac{2}{n}} \bullet \dots \bullet e^{-\frac{k-1}{n}} \right] = 1 - e^{-\frac{k(k-1)}{2n}} \end{aligned}$$

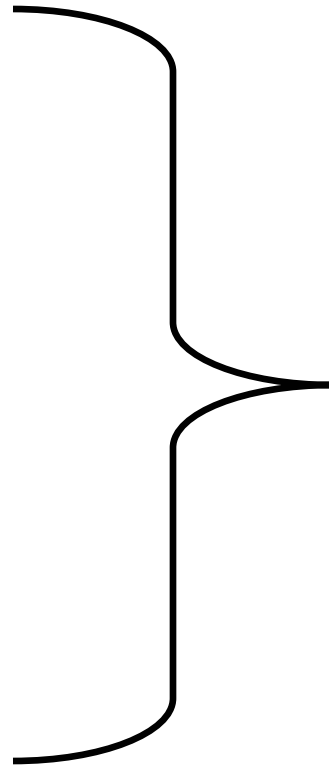
Solution to the general problem

$$\begin{aligned} P(n, k) > 0.5 \\ \text{implies} \end{aligned} \quad \frac{1}{2} = 1 - e^{-\frac{k(k-1)}{2n}} \Leftrightarrow e^{-\frac{k(k-1)}{2n}} = \frac{1}{2}$$
$$\Leftrightarrow \frac{k(k-1)}{2n} = \ln 2$$

For large k , $(k-1)k \approx k^2$, we obtain

$$k \approx \sqrt{(2 \ln 2)n} = 1.18\sqrt{n} \approx \sqrt{n}$$

End Math



Repeating Blocks

- Repeating ciphertext blocks leak information in ECB, CBC
 - What is the probability of two ciphertext blocks are the same in ECB mode, assuming that each plaintext block occurs with the same probability?
 - What is the probability of two ciphertext blocks are the same in the CBC mode, assuming that IV is picked randomly?
 - Why we say CBC is more secure than ECB?

Time Space tradeoff

- Trading off space vs time in attacking double DES is now part of Homework 2