Materials provided on midterm exam

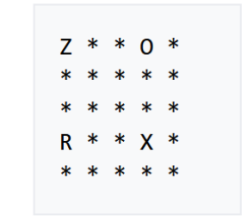
- The following slides contain figures that will be provided on the midterm exam (if they are needed)
- Facts found in this slide presentation do not need to be memorize, though you may need to remember how to make use of them

Security lattice

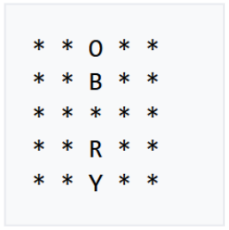
- A lattice is a set L equipped with a partial ordering ≤ such every two elements a, b ∈ L has a least upper bound a ∨ b and a greatest lower bound a ∧ b. A finite lattice must have top and bottom elements.
- take a set of classifications H and linear ordering ≤H
- take a set C of categories; compartments are subsets of C
- security levels are pairs (h, c) with h ∈ H and c ⊆ C
- ordering (h1, c1) ≤ (h2, c2) ⇐⇒ h1 ≤ h2, c1 ⊆ c2 gives a lattice.

Rules for Playfair

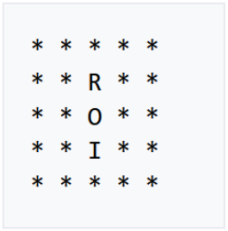
- **Rectangle**: pick from same row but opposite corner
- **Column**: pick letter one row down, wrapping if necessary.
- **Row**: pick letters one step to right, wrapping if necessary.



Hence, OR → ZX

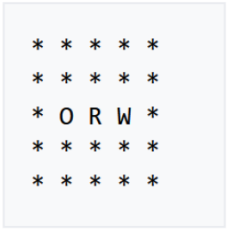


Hence, OR → BY



Hence, OR → IO

Hence, OR → YZ



Hence, OR → RW

Letter to number mappings

- For mono-alphabetic cyphers:
  - Mappings between numbers and letters will be provided
  - Key offsets will be expressed as both letters and numbers (if possible) such as Cesar key 3 (a->d)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26