Special course of a natural scientific contents, ½ year

``The number theory and cryptography’’

Professor V.N.Chubarikov

1. The number theory: elementary properties of integers, indicator of an integer, congruencies an integer modulo, the Fermat’s simple theorem, the Euler’s totient function and the Euler’s theorem for any integer modulo, the converse of Fermat’s simple theorem, primitive roots an integer modulo,

the unique factorization theorem, checking to a primality of a number, algorithms for factorization of an integer.

1. The basic notations of cryptography. Symmetric and asymmetric schiffer-system. Algorithm of RSA. The problem of the discrete logarithm.
2. Cryptograthical protocols. Hash-function. Protocol of bossing a coin on phone. The problem of a rucksack packing and it’s the system of schiffering. Digital signature.
3. An information theory and a coding theory. Main problems. The alphabetic coding. The Shannon and Gilbert—Moore a prefix codes.
4. Finite fields. Irreducible polynomials. Cyclic codes.
5. Recurrent relations. Fibonachi sequence. Linear recurrent equations. Recurrent relations in finite fields.
6. The arithmetical way to the problem of a distortion of signs in simple replacement schiffer.