Zápočtový test z předmětu 11Y2KK

Datum: 23. ledna 2006, 15:30 (A)

Jméno a příjmení:

Skupina:

Otázka 1

Dekomprimujte posloupnost znaků, komprimovanou algoritmem LZW podle zadání na tabuli. Abeceda je $\{\mathsf{A} \to 0, \mathsf{B} \to 1, \mathsf{C} \to 2, \ldots \mathsf{Z} \to 25\}$. [5 bodů]

Otázka 2

Nalezněte generující polynom stupně 4 pro binární cyklický kód délky 7. Napište generující matici a kontrolní polynom. [5 bodů]

Otázka 3

Dešifrujte následující kousek české dětské písničky, zapsané bez diakritiky v abecedě $A = \{\mathsf{ABCDEF} \ldots \mathsf{XYZ}\}$. Využijte toho, že mezery v šifrovaném i dešifrovaném textu si odpovídají a že šifrovací transformace zachovává frekvenci znaků. V modulární aritmetice zapište výslednou transformaci z nešifrovaného na šifrovaný text.

QIPE FEFOE GXCVM NEFOE E HIHIGIO NIRSQ HZI [5 bodů]

Otázka 4

Vysvětlete princip asymetrických šifer. Popište, jak lze urychlit výpočet kongruence $x \equiv a \pmod{m}$ pro velká m v případě, že m lze rozložit na součin nesoudělných čísel. [5 bodů]

Zápočtový test z předmětu 11Y2KK

Datum: 23. ledna 2006, 15:30 (B)

Jméno a příjmení:

Skupina:

Otázka 1

Dekomprimujte posloupnost znaků, komprimovanou algoritmem LZW podle zadání na tabuli. Abeceda je $\{\mathsf{A} \to 0, \mathsf{B} \to 1, \mathsf{C} \to 2, \ldots \mathsf{Z} \to 25\}$. [5 bodů]

Otázka 2

Nalezněte generující polynom stupně 4 pro binární cyklický kód délky 7. Napište generující matici a kontrolní polynom. [5 bodů]

Otázka 3

Dešifrujte následující dvojverší z dílny dvojice Vodňanský-Skoumal. Text je zapsaný bez diakritiky v abecedě $A = \{\mathsf{ABCDEF} \ldots \mathsf{XYZ}\}$. Využijte toho, že mezery v šifrovaném i dešifrovaném textu si odpovídají a že šifrovací transformace zachovává frekvenci znaků. V modulární aritmetice zapište výslednou transformaci z nešifrovaného na šifrovaný text.

QJKVGQ PK VGT VXULKYUX? PK NU VRTE QUSVXKYUX. [5 bodů]

Otázka 4

Vysvětlete princip symetrických šifer. Popište jednotlivá stádia šifry DES. [5 bodů]

Frekvenční tabulka českých textů

A 0.104	B 0.030	C 0.021	D 0.072	E 0.139
F 0.003	G 0.000	H 0.017	I 0.026	J 0.049
K 0.077	L 0.037	M 0.054	N 0.033	O 0.127
P 0.035	Q 0.000	R 0.028	S 0.037	T 0.035
U 0.028	V 0.033	W 0.000	X 0.000	Y 0.005
Z 0.007				

Frekvenční tabulka anglických textů

A 0.081	B 0.014	C 0.038	D 0.040	E 0.118
F 0.024	G 0.017	H 0.060	I 0.073	J 0.000
K 0.005	L 0.040	M 0.023	N 0.068	O 0.076
P 0.024	Q 0.001	R 0.058	S 0.074	T 0.090
U 0.029	V 0.009	W 0.018	X 0.002	Y 0.019
Z 0.001				